Commissariat
à la protection de
la vie privée du Canada

Vie privée et cybersécurité

Mettre l'accent sur la protection de la vie privée dans les activités de cybersécurité

Décembre 2014

Table des matières

Résumé

Le présent rapport porte sur les intérêts communs et les tensions entre la vie privée et la cybersécurité. On y examine comment les défis au chapitre de la cybersécurité touchent également la protection de la vie privée et des données, et comment les politiques en matière de cybersécurité peuvent influer sur la vie privée. On y souligne en outre de quelle façon la gouvernance et la sécurité du cyberespace constituent des enjeux internationaux. Enfin, le rapport établit des orientations stratégiques clés dans le but de susciter le dialogue sur la cybersécurité en tant qu'élément important de la protection de la vie privée en ligne.

Introduction

Le « cyberespace » se trouvant désormais au centre de l'infrastructure mondiale de l'information et des communications, sa sécurité est devenue une priorité plus urgente pour les entreprises et les gouvernements à l'échelle internationale[1]. En fait, la stratégie *Canada numérique 150*, lancée en avril 2014, vient parachever la stratégie du Canada en matière de cybersécurité en faisant de la protection des Canadiens l'un de ses cinq piliers[2]. Selon le document *Stratégie de cybersécurité du Canada* (la *stratégie*) datant de 2010, 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[3] ». Bien que le mot de « cybersécurité » ne soit pas défini dans la *stratégie*, on considère généralement qu'il désigne toutes les mesures adoptées pour protéger les renseignements électroniques et l'infrastructure qui les accueille[4].

Les technologies omniprésentes, interconnectées et qui offrent un accès facile à Internet font désormais partie intégrante de notre quotidien. De ce fait, nous dépendons de plus en plus du cyberespace pour les interactions sociales, économiques et politiques. Le Web constitue une plateforme pour tout un éventail de secteurs et de services touchant les infrastructures essentielles, notamment les soins de santé, l'alimentation et l'eau, les finances, les technologies de l'information et des communications, la sécurité publique, l'énergie et les services publics, le secteur de la fabrication, le transport et le gouvernement[5]. La connectivité du cyberespace contribue à l'augmentation de tous ces secteurs d'infrastructure essentiels et par conséquent, elle est vitale pour la croissance économique future du Canada[6].

Par ailleurs, l'environnement Internet fait de plus en plus souvent l'objet de menaces sophistiquées et ciblées; notre dépendance croissante au cyberespace crée de nouvelles et importantes vulnérabilités[7]. Le risque est décuplé par un certain nombre de facteurs : plus de données électroniques précieuses sont stockées et traitées à très grande échelle, la plupart du temps dans l'infonuagique; de puissants appareils numériques portables comme les téléphones intelligents, les tablettes numériques et les ordinateurs portables font de plus en plus partie de toutes les facettes de notre vie; les renseignements sont échangés, combinés et liés à d'autres renseignements à une plus grande fréquence; les relations avec des tiers (par exemple, la sous-traitance à un fournisseur de services en nuage) sont monnaie courante. À moins que les composantes soient toutes aussi sûres les unes que les autres, c'est le système en entier qui est vulnérable, les cybercriminels sachant souvent très bien comment exploiter les faiblesses du cyberespace.

Par exemple, en 2011, le Canada a subi une importante atteinte à la sécurité quand les systèmes informatiques de trois ministères clés du gouvernement fédéral ont été infiltrés[8]. Même si aucun renseignement personnel n'a, semble-t-il, été compromis au cours de l'attaque, les pirates ont pu voler des documents hautement confidentiels et ils ont obligé les ministères à se retirer d'Internet pendant des mois[9]. En 2012, le vérificateur général du Canada signalait que la réaction du gouvernement à cette atteinte à la sécurité de 2011 a démontré que les systèmes étaient clairement vulnérables et que les pratiques exemplaires

en matière de sécurité de l'information n'étaient pas appliquées de manière uniforme[10]. Le vérificateur général indiquait également que jusqu'alors, la mise en œuvre de la *stratégie* avait été lente et qu'en conséquence, la capacité du pays de protéger le cyberespace était extrêmement sous-développée[11]. Plus récemment, en 2014, une grande part du monde virtuel s'est trouvé aux prises avec « Heartbleed », un bogue de sécurité qui a mis en évidence la vulnérabilité d'un processus de cryptage couramment utilisé. Ce bogue était susceptible compromettre les noms d'utilisateur, mots de passe et autres éléments de contenu confidentiels de divers sites Web, notamment des sites populaires de médias sociaux, des fournisseurs de services de messagerie électronique sur le Web et un certain nombre de sites commerciaux électroniques[12]. Plus récemment encore, le logiciel malveillant « Blackshade » a permis la capture de renseignements sur l'ordinateur d'une victime, notamment des touches de frappe, photographies, documents et mots de passe, pour avoir accès à des comptes en ligne. Ces incidents nous ont portés à réfléchir à la fragilité d'Internet et du caractère nécessaire de la cybersécurité.

Le *Plan d'action 2010-2015 de la Stratégie de cybersécurité du Canada* (le *Plan d'action*), rendu public en avril 2013, résume les progrès accomplis à ce jour ainsi que les plans continus du gouvernement pour mettre en œuvre la *stratégie*, laquelle a été bonifiée par la publication en avril 2014 de *Canada numérique 150,* qui repose sur cinq piliers : un Canada branché, un Canada protégé, les possibilités économiques, le gouvernement numérique et le contenu canadien[13]. Depuis 2010, le gouvernement du Canada a structuré sa *stratégie* et son *Plan d'action* autour de trois piliers : 1) sécuriser les systèmes du gouvernement fédéral, 2) nouer des partenariats pour protéger les cybersystèmes essentiels à l'extérieur du gouvernement fédéral, et 3) aider les Canadiens à se protéger en ligne[14]. Le volet visant à sensibiliser la population est celui qui, à ce jour, a reçu l'attention la plus soutenue. Depuis le lancement de la *stratégie*, le gouvernement du Canada s'est concentré en priorité sur la sensibilisation et la mobilisation du public, indiquant aux Canadiens comment protéger leurs renseignements personnels dans la sphère numérique[15].

Par exemple, puisque le secteur privé est responsable en grande partie de la cybersécurité, la majorité des renseignements générés et stockés dans le cyberespace ne sont pas sous le contrôle des utilisateurs, mais entre les mains de nombreux fournisseurs du secteur privé et de tiers. Étant donné que les infrastructures essentielles sont aussi largement contrôlées par le secteur privé au Canada[16], le deuxième pilier de la *stratégie* et du *Plan d'action* reconnaît que bon nombre des risques et des répercussions des cyberincidents sont partagés entre le secteur public et le secteur privé.

La protection de la vie privée et la cybersécurité devraient être considérées comme des éléments interreliés : étant donné que des quantités toujours plus grandes de renseignements personnels sont traités et stockés en ligne, la protection de la vie privée repose de plus en plus sur la mise en œuvre efficace par les organisations de mesures de cybersécurité pour protéger les renseignements personnels tant au moment de leur transit que lorsqu'ils sont stockés[17]. Dans certains cas, les mesures de cybersécurité sous-tendent les infrastructures essentielles qui protègent les données, ce qui, du coup, protège les renseignements personnels.

Toutefois, à l'instar de nombreuses mesures de sécurité, certains efforts liés à la cybersécurité peuvent également constituer une menace pour la vie privée; la relation entre ces deux éléments n'est pas en totale harmonie. Les activités de cybersécurité peuvent exiger une surveillance constante des activités sur un réseau pour détecter les anomalies et les menaces, et parfois une surveillance de cette nature suppose la saisie et l'analyse de quantités énormes de renseignements personnels.

1. Les défis de la cybersécurité

Dans son rapport paru en janvier 2014, le Forum économique mondial examine le besoin d'adopter de nouvelles méthodes permettant d'accroître la résilience à l'égard des cyberattaques, et suggère que

l'incapacité à sécuriser efficacement le cyberespace pourrait se traduire par des pertes combinées d'environ 3 000 milliards de dollars américains d'ici 2020[18]. Cependant, bon nombre des défis liés à la cybersécurité s'appliquent également à la protection de la vie privée et des données. La cybersécurité ne constitue d'aucune façon un problème immuable comportant une solution permanente. Les menaces qui pèsent sur les renseignements dans le cyberespace évoluent rapidement, et plus récemment, elles se sont propagées à d'autres voies de communication telles que les médias sociaux et les technologies mobiles. Tandis que les organisations s'efforcent de suivre les changements créés par les technologies innovatrices, les pratiques sociales ainsi que les menaces en perpétuelle évolution, les données produites, colligées et stockées à très grande échelle peuvent devenir vulnérables à ces cybermenaces. Voici quelques-uns des défis émergents en matière de protection des données et de cybersécurité.

a) Complexité de l'« environnement branché »

L'évolution continue du cyberespace en tant qu'univers entièrement électronique créé à partir des réseaux interconnectés en parallèle avec notre environnement physique se caractérise par une quantité énorme de données. L'économie moderne dépend de plus en plus d'une vaste quantité de données numériques générées par les opérations financières, les communications, les activités de loisirs, les voyages, les achats, l'exploration du Web et des centaines d'autres activités de tous les jours[19]. Des éléments de données sont sans cesse combinés, reliés, comparés et associés à d'autres renseignements tandis que les organisations tentent de tirer profit de la valeur qu'ils représentent et d'offrir des services nouveaux et améliorés à leurs utilisateurs. Les systèmes électroniques et les réseaux numériques qui permettent ces opérations et ces communications consignent également nos préférences et d'autres détails personnels, et suivent nos activités en ligne et de plus en plus, nos déplacements physiques. Le volume de données générées dans le cyberespace ne peut que croître de façon exponentielle une fois que l'« Internet des choses » se concrétisera et que des capteurs dans les appareils signaleront de façon autonome le lieu, la situation et l'environnement, fournissant des mises à jour en temps réel ou contribuant à surveiller ou à contrôler les dispositifs à distance[20].

Le cyberespace est devenu intrinsèquement complexe à gérer, et le sécuriser constitue un défi. La connectivité constante et accrue, au moyen d'un éventail toujours plus grand de dispositifs mobiles et de services disponibles, les relations avec de tierces entreprises, les infrastructures de services informatiques infonuagiques, les accords de partage d'information et les autres processus opérationnels automatisés ou intégrés dans le cyberespace sont autant d'éléments qui continuent de comporter des risques tant pour la cybersécurité que la vie privée. Les menaces dans le cyberespace continueront de cibler les maillons les plus faibles de tout réseau complexe de relations d'affaires ou de processus gouvernementaux, ce qui signifie que les acteurs dans le domaine de la cybersécurité devront exercer un rôle commun dans la protection de l'infrastructure et de l'information qui y circule.

b) Sophistication croissante de la menace

Les menaces en ligne sont peut-être invisibles, mais leurs effets sont tout à fait tangibles et les systèmes interconnectés qui sont accessibles à l'échelle planétaire sont vulnérables de manière inhérente. À mesure que la masse des renseignements qui circulent dans le cyberespace s'est accrue, leur valeur a également augmenté pour les entreprises, les gouvernements et les personnes aux intentions malveillantes. Nos données laisse désormais une plus grande empreinte numérique, nous exposant davantage aux cybermenaces[21]. Là où il y a une possibilité de profit, il y a généralement un marché pour les activités criminelles, mais comme le signale Gabriella Coleman, le piratage[22] et la cybercriminalité se sont également « professionnalisées », devenant ainsi beaucoup plus sophistiquées[23]. Les menaces parrainées, conduites ou approuvées par certains pays, sont également de plus en plus courantes[24]. On les appelle parfois des menaces persistantes avancées (MPA) et bien souvent, elles sont le fait de personnes instruites et dotées de ressources appréciables qui se concentrent sur le vol de secrets, incluant le vol de propriété intellectuelle[25].

Ronald Deibert, directeur du Canada Centre for Global Security Studies and Citizen Lab, à la Munk School of Global Affairs, Université de Toronto, explique que la cybercriminalité augmente en fréquence et en complexité pour plusieurs raisons : [traduction] « Premièrement, la présence en ligne, qu'il s'agisse de personnes, d'entreprises, d'organisations ou de gouvernements, augmente rapidement et du coup, multiplie la base des cibles potentielles. Deuxièmement, nos façons de communiquer et d'échanger de l'information en ligne ont considérablement changé au cours des dernières années avec la croissance des réseaux sociaux, l'informatique en nuage et les formes mobiles de connectivité. Nous partageons plus de données entre nous, nous confions leur circulation à un tiers sur lequel nous n'avons aucun contrôle immédiat, et nous cliquons de plus en plus souvent sur des liens et des documents offerts par des plateformes et des services de réseaux sociaux[26]. » Troisièmement, selon M. Deibert, puisqu'il est rare que les entreprises révèlent publiquement les atteintes à la sécurité, pour des raisons de concurrence et pour préserver leur réputation, on sait peu de choses sur la façon dont les attaques sont menées, ce qui peut en fin de compte nuire aux efforts de cybersécurité[27].

c) Les menaces se déplacent vers la sphère mobile

Au cours des trois prochaines années, il y aura plus de téléphones cellulaires utilisés que de personnes sur la Terre[28]. Nos dispositifs mobiles peuvent contenir une mine de renseignements personnels précieux. Les gens se déplacent partout avec leur téléphone mobile et les utilisent pour des raisons des plus variées : communiquer avec leurs amis, accéder à leurs courriels, prendre des photos et faire des vidéos puis les télécharger sur Internet, jouer à des jeux, évaluer les distances, localiser des magasins et des restaurants à proximité, établir un itinéraire vers un lieu précis, accéder à un compte bancaire, naviguer sur le Web, surveiller leur santé et leurs activités physiques, se remémorer un rendez-vous ou consigner des listes de tâches. Les organisations s'efforcent toutes de rejoindre les consommateurs et les clients sur les appareils portables qu'ils utilisent tous les jours mais, parallèlement à la commodité dont bénéficient les consommateurs, se profile la possibilité de nouvelles vulnérabilités ou cybermenaces.

Récemment, l'International Cyber Security Protection Alliance (ICSPA) a publié une étude sur la cybercriminalité où l'on souligne que les communications mobiles et les services infonuagiques constituent aujourd'hui les nouvelles cibles de cybercriminalité[29]. Selon cette étude, la multiplication exponentielle du nombre de maliciels visant les appareils mobiles représente l'un des principaux enjeux sur lesquels l'industrie devra se pencher. Les maliciels peuvent facilement infecter un dispositif mobile au moyen d'applications malveillantes téléchargées dans les boutiques d'applications des téléphones intelligents et qui apparaissent sécuritaires à première vue[30]. Qui plus est, l'accès gratuit au Wi-Fi dans des lieux publics peut également augmenter les risques d'interception des données par un tiers[31]. Les maliciels peuvent cibler des dispositifs mobiles lors de leur utilisation du protocole NFC (communications en champ proche) et compromettre la fonction de paiement sans contact[32]. L'étude de l'ICSPA conclut que les logiciels malveillants visant les appareils mobiles représentent une importante menace émergente dans le cyberespace. Néanmoins, et bien que les cybercriminels mettent au point des maliciels plus efficaces pour cibler les appareils mobiles, les taux réels d'infection de ces appareils sont faibles à l'heure actuelle car la distribution des maliciels aux dispositifs mobiles n'est pas encore perfectionnés[33]. On peut s'attendre à ce que cette situation change sous peu.

Comme les cybermenaces ciblent de plus en plus souvent les dispositifs mobiles, la protection des données n'en devient que plus essentielle. Les communications et les transactions au moyen des dispositifs mobiles sont davantage reliées aux utilisateurs eux-mêmes; les capteurs intégrés peuvent être activés afin de localiser les appareils avec une extrême précision, et les fonctions incorporés aux appareils ou les applications téléchargées peuvent suivre à la trace, consigner et stocker des renseignements personnels ainsi que télécharger les listes de contacts, les messages et les transactions effectuées. Confrontés à cette escalade de risques, l'industrie des dispositifs mobiles, les entreprises et les concepteurs d'applications ont une responsabilité accrue d'assurer la sécurité des plateformes et des systèmes dorsaux où tant de renseignements personnels sont recueillis, manipulés et stockés.

d) Le paradoxe des « mégadonnées » : s'agit-il d'un risque accru ou d'une solution?

On peut définir les « mégadonnées » comme de vastes dépôts de renseignements rassemblés à la fois à partir de sources traditionnelles et, de plus en plus, de nouveaux points de cueillette (p. ex. les données sur le Web, les données de capteur, les données documentaires et les données sur le temps et les lieux recueillies dans les médias sociaux)[34]. Il arrive souvent qu'on vante le savoir dérivé de l'analyse des mégadonnées comme la solution à tous les problèmes[35]. Toutefois, dans une optique de cybersécurité, cette approche axée sur les données soulève deux questions distinctes : comment protéger les renseignements dans le contexte de mégadonnées et comment utiliser la nouvelle analytique des données pour faire le tri dans les renseignements du réseau, y compris les renseignements personnels, afin de prédire les incidents ayant trait à la sécurité[36].

Autant les données (qu'il s'agisse ou non de mégadonnées) sont considérées comme un actif commercial précieux, autant elles sont probablement tout aussi précieuses pour les pirates informatiques. Les atteintes à la sécurité auront possiblement des conséquences graves sur les fournisseurs de mégadonnées, étant donné qu'il est relativement nouveau pour la plupart des organisations de recourir à ce type de données et qu'on ne comprend pas encore très bien les vulnérabilités et les risques qui s'y rattachent. Les organisations qui décident de recourir à l'analytique des mégadonnées pourraient créer de nouvelles vulnérabilités potentielles en matière de sécurité, ou des occasions de saisir des données malveillantes[37]. De plus, les mégadonnées engendrent des « méga-mégadonnées »; à mesure que la capacité de colliger des données augmente, la tentation d'en recueillir davantage augmente également.

Les partisans de l'analyse des mégadonnées ont affirmé qu'elles pourraient jouer un rôle clé dans la détection des cybermenaces à un stade précoce, grâce à une analyse complexe des modèles et par l'association et l'analyse des sources de données multiples[38]. De plus, on a vanté le pouvoir des mégadonnées à titre d'outil essentiel de résolution de problème qui permet d'améliorer la sécurité publique[39] et les soins de santé[40] ainsi que d'économiser de l'énergie[41]. Par ailleurs, la complexité inhérente à ces mêmes points de données multiples et leur intégration à l'échelle des plateformes rendront encore plus complexe le processus de protection nécessaire à la sauvegarde des renseignements. Bien entendu, de par le fait que l'analytique des mégadonnées soulève des inquiétudes, car elle sous-entend souvent une collecte sans restriction de données et une analyse complexe pouvant jeter un éclairage très intime sur nombres d'individus. C'est également un processus susceptible de motiver des utilisations secondaires déraisonnables de renseignements personnels. Peter Wood, président et directeur général de First Base Technologies LLP et membre du groupe consultatif sur la sécurité de la section de Londres de l'ISACA, explique que le nœud du problème est le fait que le volume et la vitesse associés aux mégadonnées repoussent les frontières des responsabilités actuelles en matière de sécurité de l'information et comportent de ce fait de nouveaux risques et de nouveaux défis[42].

e) Pour beaucoup, la préparation aux cas d'atteinte à la vie privée ne constitue toujours pas une priorité

Ces dernières années, de plus en plus d'atteintes à la vie privée ont été signalées, et les conséquences de ces atteintes peuvent parfois être graves pour les personnes touchées. Les gouvernements et le secteur privé partagent bon nombre des risques et des conséquences des incidents sur Internet, mais la plupart du temps, il incombe d'abord au secteur privé d'affronter ces menaces étant donné que les entreprises contrôlent la plupart des infrastructures de télécommunications[43]. Plusieurs rapports récents ont indiqué qu'un grand nombre d'entreprises ne sont pas préparées aux cyberattaques, y sont indifférentes, et n'ont pas de plan d'urgence adéquat[44].

Au cours des dernières années, les entreprises canadiennes ont été confrontés aux problèmes liés à la cybersécurité[45]. De manière générale, l'étude de l'ICSPA sur l'impact de la cybercriminalité a révélé d'importantes lacunes dans les plans de préparation des entreprises canadiennes pour lutter contre la cybercriminalité, mais suggère que les grandes entreprises seraient toutefois mieux préparées à répondre aux

cybermenaces en constante évolution[46]. Les maliciels, les attaques virales, le sabotage de données ou de réseaux, la fraude financière, l'hameçonnage, l'ingénierie sociale, le vol d'ordinateurs ou de dispositifs portables, l'accès non autorisé à un site Web ou son utilisation abusive, l'usage à des fins mal intentionnées de réseaux sociaux par les employés, le déni de service, la fraude liée aux télécommunications, ainsi que les menaces persistantes avancées constituent les principales cybermenaces (selon les réponses recueillies auprès des entreprises ayant répondu au sondage)[47]. Selon l'étude, la plupart des entreprises canadiennes ayant participé à l'enquête (69 %) n'avaient pas mis en place de procédures de réponse en cas de cyberattaque, et seulement 22 % ont indiqué avoir recours à un processus d'évaluation des risques pour déterminer leurs points faibles[48]. Cette situation est préoccupante, d'autant plus que selon les résultats de l'enquête, les entreprises canadiennes sont fréquemment touchées par la cybercriminalité : 69 % ont indiqué avoir subi une attaque d'un type ou d'un autre dans une période de douze mois.

Alors que les entreprises semblent mal préparées pour répondre aux cybermenaces et aux atteintes à la vie privée, les gens souhaitent savoir s'ils peuvent être touchés par ce type d'attaque et à quel moment. Selon l'enquête auprès des Canadiens menée par le Commissariat en 2013, les répondants ne savaient pas au juste si on les avertirait que des renseignements personnels fournis à une organisation ont été perdus, volés ou révélés de façon non intentionnelle : 59 % étaient d'avis que c'était peu probable; 41 %, que c'était probable. Toutefois, pratiquement tous les Canadiens (97 %) qui ont participé à l'enquête ont déclaré vouloir être informés de la situation[49], ce qui semble indiquer qu'ils appuieraient des améliorations à la façon dont les organisations gèrent la sécurité de l'information et la réponse en cas d'atteinte à la vie privée. Dans une enquête auprès des entreprises commandée par le Commissariat en 2014, 58 % d'entre elles ont indiqué ne pas disposer de lignes directrices en cas d'atteinte concernant les renseignements personnels de leurs clients[50]. L'absence de préparation organisationnelle et le peu de priorité accordée aux répercussions potentielles semblent indiquer que la préparation en cas d'atteintes ne constitue pas encore une priorité opérationnelle.

f) Conformité et gestion du risque

Les organisations doivent respecter plusieurs lois et règlements pour mener leurs activités à l'intérieur de juridictions spécifiques ou entre diverses juridictions. Toutefois, quand il s'agit de sécurité, une approche mécanique en matière de conformité ne signifie pas nécessairement que l'organisation est protégée contre les risques[51]. De fait, en focalisant sur une approche de la conformité basée sur un « cochez les cases », une entreprise peut s'exposer à un risque accru dû à un faux sentiment de sécurité alors qu'une gestion appropriée du risque exige un examen attentif pour déterminer là où il est nécessaire de prendre des mesures de sécurité supplémentaires[52]. Une stratégie de gestion du risque complète naturellement les obligations en matière de conformités. Le défi pour les organisations est de comprendre que la sécurité n'est pas une simple affaire de respect des normes de conformité minimales; elles doivent adopter des mesures efficaces de gestion du risque et de mise en œuvre dynamique de la sécurité[53].

2. Les développements stratégiques en matière de cybersécurité

La cybersécurité constitue une question stratégique incroyablement complexe et mouvante. Aucun pays ni aucune organisation ou personne n'est entièrement à l'abri des risques dans l'univers virtuel, et les méthodes pour se protéger de ces menaces peuvent varier considérablement selon les valeurs et les décisions qui sous-tendent les activités de cybersécurité[54]. En fait, la question de la cybersécurité touche à des enjeux plus vastes liés à la gouvernance d'Internet. Deux points de vue divergents sont observés quant à la réglementation liée à la cybersécurité : l'un favorise une approche harmonisée en matière de gouvernance, laquelle protège l'ouverture, les renseignements personnels et l'interopérabilité à l'échelle des régions – il s'agit de l'approche des « biens communs ouverts » –, tandis que l'autre favorise un contrôle gouvernemental et une réglementation plus stricts – c'est l'approche de la « communauté protégée »[55].

On a fait valoir que la cybersécurité est bien plus qu'une question technique puisqu'elle touche la sécurité d'un écosystème complet de communication[56]. À cet égard, bien que la cybersécurité nécessite inévitablement certains développements techniques, elle exigera aussi l'élaboration de normes sociales, la collaboration entre pays et un cadre de réglementation regroupant de multiples intervenants. Lorsque les orientations en matière de cybersécurité seront évaluées, il sera essentiel que l'on reconnaisse dans le cadre des débats les liens que la cybersécurité entretient avec la protection des données, la confiance et la protection de la vie privée. La section qui suit examine les développements stratégiques relatifs à la cybersécurité et ainsi que des considérations relevant de la politique étrangère.

a) Intendance et sécurisation[57]

Alors que les politiques en matière de cybersécurité sont en cours de développement au niveau national, la protection de la vie privée risque d'être subordonnée aux objectifs liés à la sécurité nationale et à la sécurité publique dans le cadre des réponses élaborées pour contrer les cybermenaces[58]. La politique de cybersécurité pourrait donc permettre ce que Deibert décrit comme une [traduction] « sécurisation du cyberespace – la transformation du cyberespace en question de sécurité nationale »[59]. À une époque où la sécurité nationale sert souvent à justifier une intrusion extraordinaire dans la vie privée des individus, il faudra veiller de près à ce que les stratégies et activités de cybersécurité ne conduisent pas à la mise en œuvre de régimes de surveillance visant à un monitorage et une analyse illimités et ininterrompus des renseignements personnels.[60] Les efforts en matière de cybersécurité ne devraient pas étendre la surveillance au point d'empiéter sur la vie privée des individus, les libertés civiles ou d'autres valeurs démocratiques[61]. Les gouvernements doivent établir les mécanismes de vérification et de contrôle nécessaires pour respecter les normes de protection de la vie privée auxquelles nous souscrivons en tant que société.

Une approche d'*intendance* à la cybersécurité peut être considérée comme un contrepoids à ce modèle, où [traduction] « les gouvernements, les ONG, les forces armées, les organismes d'application des lois et les agences du renseignement, les entreprises du secteur privé, les programmeurs, les technologues et les utilisateurs moyens doivent tous jouer un rôle essentiel et interdépendant de gardien du cyberespace »[62]. Ce concept d'intendance de la cybersécurité reconnaît que le cyberespace n'appartient à personne en particulier, mais que tous ont un rôle important à jouer dans l'édification de ses bases et dans les enjeux reliés à son évolution.[63].

Cette autre approche aborde la cybersécurité comme une responsabilité partagée en raison des interconnexions et de l'interdépendance dans le cyberespace, ainsi que du rôle que toutes les organisations doivent jouer pour s'assurer que leurs actions n'entraînent pas de risque pour la sécurité dans le cyberespace en général ou un non-respect des principes de protection de la vie privée.[64] L'approche axée sur l'intendance exige également que tous les intervenants impliqués dans le domaine de la cybersécurité soient en mesure de rendre compte: [traduction] « Pour assurer la sécurité du cyberespace, il faut renforcer les balises qu'on impose au pouvoir et non les assouplir, ce qui suppose des mécanismes régulateurs applicables tant aux gouvernements, aux organismes chargés de l'application de la loi, aux agences de renseignement qu'au secteur privé[65] ». Et puisque le secteur privé détient de grandes quantités de renseignements personnels, il est logique de s'attendre à ce qu'il assume certaines responsabilités concernant la protection de l'infrastructure du cyberespace ainsi que les renseignements personnels qui y circulent.

Les deux approches, celle d'un contrôle gouvernemental intégré et celle plus large d'intendance, ont des avantages et peuvent même se compléter l'une l'autre.

b) La gouvernance du cyberespace et la sécurité constituent un enjeu international

Étant donné que l'information qui circule dans le cyberespace n'est pas limitée par des frontières nationales, [traduction] « les partenaires d'échange de données et l'endroit où ces données résident dans le cyberespace

constituent par définition un enjeu international »[66]. De ce fait, les citoyens de tous les pays sont confrontés aux mêmes risques à l'égard de leur droit à la protection de leurs renseignements personnels. Les questions de cybersécurité et de protection de la vie privée sont des questions internationale qui exigent une réponse internationale.

Le *Plan d'action* invite le ministère des Affaires étrangères, du Commerce et du Développement à élaborer une politique étrangère du Web pour s'assurer que les activités menées dans le cyberespace soient conformes aux objectifs plus vaste de politique étrangère, de commerce international et de sécurité[67]. Les groupes internationaux tels que le G8, l'Organisation pour la sécurité et la coopération en Europe (OSCE) et l'Organisation de coopération et de développement économiques (OCDE) élaborent des principes en appui au droit d'accès au cyberespace, à son ouverture, à la liberté d'expression et au droit à la protection de la vie privée des utilisateurs. Toutefois, ces mêmes principes peuvent être en porte-à-faux avec les objectifs de sécurité nationale ou de sécurité publique, ainsi qu'avec les intentions des fournisseurs qui créent des produits de cybersécurité dotés de capacités intégrées visant à suivre les utilisateurs, surveiller la fréquentation des réseaux et filtrer le contenu[68].

À mesure que se développent les orientations stratégiques en matière de cybersécurité, les autorités de protection des données personnelles et de la vie privée ont un rôle à jouer afin de s'assurer que les politiques en matière de cybersécurité respectent le droit et les valeurs associées à la vie privée et accordent la priorité nécessaire à la protection des renseignements personnels.

Étant une des autorités de protection des données personnelles, le Commissariat est perçu comme un joueur clé qui contribue à l'élaboration de la gouvernance internationale du cyberespace, et cela grâce à ses efforts afin de s'assurer que les offres de services en ligne des entreprises internationales respectent le droit des Canadiens à la vie privée conformément aux normes canadiennes en la matière[69]. La coopération internationale dans les secteurs de la cybersécurité et de la protection de la vie privée continuera d'être essentielle pour relever les défis que pose la circulation de données entre pays et entre organisations en ce qui a trait à la sécurité et à la protection des données[70]. En 2013, Peter Hustinx, le contrôleur européen de la protection des données, a reconnu la nécessité d'aborder à un niveau international les questions de cybersécurité par le biais de normes et de mesures de coopération internationales[71]. Hustinx a aussi déclaré que « [b]ien que des mesures pour assurer la cybersécurité peuvent nécessiter l'analyse de certaines données personnelles, notamment des adresses IP qui peuvent permettre d'identifier des individus spécifiques, la cybersécurité peut jouer un rôle fondamental pour assurer le respect de la vie privée et la protection des données personnelles en ligne, à condition que le traitement de ces données soit proportionné, nécessaire et légitime[72] ».

3. Conclusion : Mettre l'accent sur la protection de la vie privée dans les activités de cybersécurité

À mesure que s'accroissent le nombre d'internautes et leur dépendance à Internet, ceux-ci compteront davantage sur la mise en œuvre efficace de mesures de cybersécurité par les organisations et la sensibilité relative à la protection des renseignements personnels de ces dernières. On trouvera ci-dessous certains secteurs clés pour lesquels une protection accrue de la vie privée pourrait contribuer au soutien, au progrès et à l'amélioration des activités de cybersécurité.

a) Intégrer des valeurs relatives à la vie privée dans les orientations stratégiques en matière de cybersécurité

Nous savons que dans une certaine mesure, le contrôle, l'enregistrement, l'exploration ou la surveillance des données créeront des tensions ou des exigences conflictuelles entre le droit à la vie privée et les efforts de

cybersécurité. Comme l'a dit en 2011 la commissaire à la protection de la vie privée du Canada par intérim, « [l]a violation de la vie privée dans le but d'assurer la cybersécurité irait à l'encontre de l'objectif de la cybersécurité[73]. » Bien que les activités de cybersécurité puissent exiger certaines mesures de surveillance pour détecter les anomalies et protéger l'infrastructure virtuelle et l'information, les stratégies et les activités de cybersécurité ne devraient pas constituer un prétexte pour élaborer des régimes de surveillance à grande échelle en vue de permettre un monitorage et une analyse sans aucune entrave des renseignements personnels. Les organismes de réglementation en matière de protection de la vie privée et ses défenseurs ont un rôle à jouer pour s'assurer que les stratégies, les principes, les plans d'action et les activités de mise en œuvre touchant la cybersécurité favorisent la protection de la vie privée à la fois comme principe directeur et comme norme durable.

Dans son Rapport sur les plans et les priorités de 2013-2014, le ministère des Affaires étrangères, du Commerce et du Développement s'est engagé à mettre en place une politique étrangère de cybersécurité pour promouvoir les intérêts du Canada liés à Internet par rapport à l'économie, à la sécurité et à la politique étrangère[74]. Cette priorité découle directement du *Plan d'action* et s'inscrit dans le plan d'ensemble du gouvernement pour mettre en œuvre la *stratégie* lancée en 2010. Le Ministère assume des responsabilités en matière de politique étrangère pour ce qui est de coordonner la participation du Canada aux efforts internationaux d'appui aux initiatives de cybersécurité, notamment la *Convention sur la cybercriminalité* de la Commission européenne, que le Canada a signée[75].

Il existe des avantages indéniables au fait d'intégrer dès le départ la cybersécurité dans les programmes et activités plutôt que d'atténuer les risques rétroactivement. En adoptant des mesures préventives pour assurer la sécurité – et en informant les consommateurs des risques potentiels et des mesures qui ont été prises pour en diminuer la portée – on peut favoriser la confiance des internautes.

b) Les approches législatives qui favorisent la préparation en matière de cybersécurité

Le secteur privé assure une responsabilité importante liée à la cybersécurité parce qu'il contrôle une très large part de l'infrastructure et de l'information dans le cyberespace. Le volume et l'éventail des renseignements personnels colligés constituent un bien précieux pour les organisations, mais également pour les malfaiteurs. Dans la course qu'elles se livrent pour innover et élaborer de nouvelles technologies, de nouveaux services et de nouvelles applications, les organisations concurrentes n'en font peut-être pas assez pour évaluer correctement le risque sur le Web. Il arrive trop souvent qu'on traite les renseignements personnels comme des marchandises que l'on contrôle, rassemble, recueille, utilise, divulgue et retient sans se soucier outre mesure des répercussions sur la vie privée. De trop nombreuses organisations prêtent le flanc aux intrusions, soit parce qu'elles n'ont pas la préparation suffisante, soit parce qu'elles sous-évaluent l'impact du piratage, et beaucoup trop souvent, elles acceptent la perte de données comme un coût inhérent à la poursuite des affaires.

Le *Plan d'action* vise à améliorer les outils législatifs afin de protéger les Canadiens dans le cyberespace. La promesse législative comprend la *Loi canadienne anti-pourriel*[76], qui est entrée en vigueur en juillet 2014, et la notification en cas de violation des données, contenue dans le projet de loi S-4, *Loi sur la protection des renseignements personnels numériques*, présenté en avril 2014.

Il ne fait aucun doute que le secteur privé est confronté à des défis de taille pour ce qui est de protéger le cyberespace. Le réseau des relations commerciales, la connectivité persistante et l'éventail toujours plus grand de dispositifs et de canaux rendent le cyberespace complexe en soi et difficile à sécuriser. Il n'empêche qu'en tant que gardien de quantités énormes de renseignements personnels, le secteur privé assume une responsabilité et un rôle partagés dans la protection de l'infrastructure du cyberespace et des renseignements personnels qui y circulent.

Il n'existe pas de solution simple aux menaces persistantes, en constante mutation, contre le droit à la vie privée dans le cyberespace. Toutes les solutions législatives doivent être examinées avec soin pour garantir leur équilibre et s'assurer qu'on peut compter sur un processus de responsabilisation par rapport à la protection des renseignements personnels. La mise en œuvre pratique de la cybersécurité suppose que l'on considère les renseignements personnels comme un bien essentiel qu'il faut protéger, qu'on définisse les vulnérabilités qui mettent ces renseignements en danger et qu'on applique des mesures de protection contre les risques circonscrits, sans pour autant nuire aux droits à la vie privée ou à d'autres valeurs telles que l'ouverture et la liberté d'expression. Le fait d'engager le dialogue avec le secteur privé sur des éléments essentiels à la mise en œuvre de la cybersécurité pourrait mettre au jour certains éléments de leur évaluation du risque et de leurs mesures de protection qui doivent toujours être renforcés.

c) Faciliter un vaste dialogue sur la cybersécurité où l'on reconnaît son importance au chapitre de la protection de la vie privée, de la confiance et de la gérance responsable des données

La complexité du cyberespace et le caractère de plus en plus sophistiqué des menaces qui pèsent sur lui exigent que les organisations multiplient les efforts pour protéger la vie privée, notamment en ce qui concerne la cybersécurité. Les mécanismes de sécurité constituent un élément clé de la capacité de protéger les renseignements personnels et la vie privée dans le cyberespace, et les mesures de protection techniques ne constituent qu'un volet du processus global de gestion du risque pour la cybersécurité et la protection des renseignements personnels. Il n'est plus suffisant de simplement respecter les exigences en matière de protection de la vie privée ou les méthodes de protection techniques. La protection des renseignements personnels exige l'application et le respect de tous les principes et règles relatifs à la vie privée pour toute la durée de vie de l'information, par exemple : agir de façon responsable et avec transparence, réduire les données au minimum, assurer l'utilisation et la divulgation appropriées des données, mettre en place des mesures de contrôle d'accès efficaces et respecter des périodes de rétention raisonnables et des méthodes de destruction sans risque.

De plus, en raison de l'interconnectivité et des risques partagés dans le cyberespace, tous les intervenants assument la responsabilité commune de façonner le cyberespace et la cybersécurité dans un esprit de confiance durable. Les efforts de cybersécurité exigeront une collaboration à l'échelle internationale et une approche de gérance garantissant la transparence des processus et des mécanismes régulateurs pour tous les intervenants concernés par les activités de cybersécurité. Les organismes de réglementation en matière de protection de la vie privée ont un rôle à jouer dans ce dialogue à grande échelle sur la gérance internationale, pour s'assurer que les efforts liés à la cybersécurité se fondent sur une approche de gestion du risque équilibrée et proportionnelle qui protège efficacement les renseignements personnels et respecte le droit à la vie privée.

Bibliographie

[1] Deibert, Ron. *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in cyberespace*. Préparé pour le Canadian Defence & Foreign Affairs Institute, août 2012.

[2] Voir la page du gouvernement du Canada *Canada numérique 150* (2014) à http://www.digitaleconomy.gc.ca/eic/site/028.nsf/fra/accueil.

[3] Stratégie de cybersécurité du gouvernement du Canada (2010), http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-fra.pdf.

[4] Il n'existe pas de définition communément reconnue de cybersécurité. ISO/IEC 27032/2012 définit la cybersécurité comme étant la protection des renseignements personnels, de l'intégrité et de la disponibilité de l'information dans le cyberespace.

[5] Consulter le site Web de Sécurité publique Canada pour obtenir une liste des secteurs d'infrastructures essentielles. http://www.securitepublique.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-fra.aspx.

[6] « *Canada and Cyberespace: Key Issues and Challenges »* (2012). Rapport préparé par SecDev Group, commandé par le ministère des Affaires étrangères, du Commerce et du Développement (MAECD).

[7] Cela est reconnu dans le *Plan d'action 2010-2015 de la Stratégie de cybersécurité du Canada* (le « Plan d'action »), lancé en avril 2013.

[8] Le ministère des Finances, le Secrétariat du Conseil du Trésor du Canada ainsi que Recherche et développement pour la défense Canada ont été touchés. Ces données ont été puisées dans « *Canada and Cyberespace: Key Issues and Challenges* » (2012). Rapport préparé par SecDev Group, commandé par le ministère des Affaires étrangères, du Commerce et du Développement (MAECD).

[9] « *Canada and Cyberespace: Key Issues and Challenges* » (2012). Rapport préparé par SecDev Group, commandé par le ministère des Affaires étrangères, du Commerce et du Développement (MAECD).

[10] Rapport – Automne 2012 – Bureau du vérificateur général (2012). Chapitre 3 — Protéger l'infrastructure canadienne essentielle contre les cybermenaces.

[11] Rapport – Automne 2012 – Bureau du vérificateur général (2012). Chapitre 3 — Protéger l'infrastructure canadienne essentielle contre les cybermenaces et « *Canada and Cyberspace: Key Issues and Challenges »* (2012). Rapport préparé par SecDev Group, commandé par le ministère des Affaires étrangères, du Commerce et du Développement (MAECD).

[12] The Heartbleed Hit List: The Passwords You Need to Change Right Now. Consulté en ligne à http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/.

[13] Voir la page du gouvernement du Canada *Canada numérique 150* (2014) à http://www.digitaleconomy.gc.ca/eic/site/028.nsf/fra/accueil.

[14] *Plan d'action 2010-2015 de la Stratégie de cybersécurité du Canada*, http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-fra.aspx.

[15] Le CPVP participe déjà à des projets qui contribuent à sensibiliser les citoyens et les petites entreprises de tout le Canada à la cybersécurité et à son importance pour la protection des renseignements personnels. En 2010, le CPVP a lancé un *outil de la protection de la vie privée à l'intention de la petite entreprise* conçu pour aider les PME à construire des plans de protection de la vie privée sur mesure. En 2011, le CPVP a élaboré une série d'articles offrant des conseils et des trucs en matière de cybersécurité pour la petite entreprise. Le CPVP a aussi travaillé en collaboration avec Sécurité publique Canada à revoir la partie de son site Web sur la cybersécurité, afin qu'il contienne des renseignements à l'intention des personnes sur la façon de se protéger. Consultez : Pensez cybersécurité. Dans la même veine, les conseils du CPVP sur les applis mobiles et des fiches de renseignements sur la protection des renseignements personnels sur les appareils mobiles : La protection de la vie privée à l'air libre : 10 conseils à suivre pour aider les particuliers à protéger les renseignements personnels sur les appareils mobiles et La protection de la vie privée à l'air libre : 10 conseils à suivre en milieu de travail pour protéger les renseignements personnels sur les appareils mobiles.

[16] Voir le blogue de Sécurité publique Canada *Pensez Cybersécurité*, 29 octobre 2013. « Alors… qu'est-ce qu'une infrastructure essentielle, de toute façon? » http://www.pensezcybersecurite.gc.ca/cnt/blg/pst-20131029-fra.aspx.

[17] Discours du commissaire : Nouvelles plateformes, nouvelles mesures de protection : protéger la vie privée dans le cyberespace (23 février 2011).

[18] Rapport du Forum économique mondial sur *Risk and Responsibility in a Hyperconnected World* (Risque et responsabilité dans un monde hyperconnecté), publié le 20 janvier 2014.

[19] Center for Applied Cybersecurity Research, Université de l'Indiana. *Roundtable on Cyber Threats, Objectives, and Responses: A Report*. Décembre 2012.

[20] Business Insider, « Everything You Need To Know About The New Internet—The 'Internet Of Things' ». Julie Bort. Publié le 29 mars 2013. Consulté en ligne le 7 octobre 2013 à http://www.businessinsider.com/what-you-need-to-know-about-the-internet-of-things-2013-3?op=1#ixzz2h3ge4p7R.

[21] Abordé dans une interview avec Ron Deibert, à l'adresse suivante : http://ww3.tvo.org/video/193823/ron-deibert-surveilling-cyberespace.

[22] On parle couramment d'« intrusion », mais il serait plus pertinent sur le plan technique de parler de « piratage ». Dans son sens premier, une « intrusion » consiste à chercher avant tout à comprendre la nature d'un système. Bien qu'on utilise le terme d'intrusion (« hacking ») tout au long de l'article, il est employé dans le sens de « piratage » c'est-à-dire qu'il s'agit d'une activité criminelle. Pour plus de renseignements sur les « intrusions » et le « piratage informatique », consultez les travaux de Gabriella Coleman, en particulier « Politics and Publics » à http://gabriellacoleman.org/wp-content/uploads/2012/08/Coleman-hacker-politics-publics.pdf ou encore « Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism » à http://steinhardt.nyu.edu/scmsAdmin/uploads/003/679/255.pdf.

[23] Google Big Tent Canada 2013, *Google Demonstration: Cyber Security in Action*, 30 mai 2013.

[24] Ibid.

[25] « Study of the Impact of Cyber Crime on Businesses in Canada ». *International Cyber Security Protection Alliance* (mai 2013), p. 33.

[26] Deibert, Ron. *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in cyberespace*. Préparé pour le Canadian Defence & Foreign Affairs Institute. Pages 11-12.

[27] Ibid.

[28] « *Canada and Cyberespace: Key Issues and Challenges* » (2012). Rapport préparé par SecDev Group, commandé par le ministère des Affaires étrangères, du Commerce et du Développement (MAECD).

[29] « Study of the Impact of Cyber Crime on Businesses in Canada ». *International Cybersecurity Protection Alliance* (mai 2013). L'étude a été parrainée par Above Security, Blackberry, Lockheed Martin et McAfee.

[30] « Study of the Impact of Cyber Crime on Businesses in Canada». *International cybersecurity Protection Alliance* (mai 2013) page 28.

[31] Ibid., page 36.

[32] McAfee 2013 Threats Predictions Report, McAfee Labs. http://www.mcafee.com/ca/resources/reports/rp-threat-predictions-2013.pdf.

[33] Ce point de vue se fonde sur cette idée que la plupart des logiciels malveillants qui ciblent les appareils Android se cachent dans les applications vendues ou cédées sans frais dans les boutiques en ligne autres que la boutique officielle « Google Play », laquelle détecte les codes malveillants. Voir Computerworld « Windows malware finds its way to Android », par Antone Gonsalves, publié le 16 août 2013. Consulté en ligne le 4 octobre 2013 à http://blogs.computerworld.com/mobile-security/22662/windows-malware-finds-its-way-android?source=CTWNLE_nlt_security_2013-08-19.

[34] « Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance ». *Centre for Information Policy Leadership*, février 2013.

[35] « Why Data Analytics is the Future of Everything », *Bloomberg TV*, 21 novembre 2013. Eric Schmidt, président exécutif de Google, et Dan Wagner, président et directeur général de Civis Analytics, examinent comment les « mégadonnées » peuvent tout changer, de la stratégie des entreprises à la façon dont les gens votent. Ils s'entretiennent avec Trish Regan, (Bloomberg – The Year Ahead) : Conférence de 2014 à l'Art Institute of Chicago. http://www.bloomberg.com/video/why-data-analytics-is-the-future-of-everything-WeneeY4LQzKJ4khYdMi9uw.html.

[36] Peter Wood. « How to tackle big data from a security point of view ». *Computer Weekly,* 4 mars 2013. Consulté en ligne le 5 septembre 2013 à http://www.computerweekly.com/feature/How-to-tackle-big-data-from-a-security-point-of-view.

[37] Ibid.

[38] Il existe une multitude de produits sur le marché, voir notamment IBM et SAS.

[39] Voir « Yes, Big Data Can Solve Real World Problems ». *Forbes*, décembre 2013 à http://www.forbes.com/sites/gregsatell/2013/12/03/yes-big-data-can-solve-real-world-problems/.

[40] Rebecca Walberg. « Value of big data in health care is measured not just in dollars, but in lives ». Financial Post, février 2014; http://business.financialpost.com/2014/02/05/value-of-big-data-in-health-care-is-measured-not-just-in-dollars-but-in-lives/?__lsa=dd3e-6a53.

[41] Michael Bendewald. « How Energy Managers can Leverage Big Data Right Now ». FacilitiesNet, avril 2013; http://www.facilitiesnet.com/energyefficiency/article/How-Energy-Managers-Can-Leverage-Big-Data-Right-Now--13976#.

[42] Peter Wood. « How to tackle big data from a security point of view ». *Computer Weekly,* 4 mars 2013. Consulté en ligne le 5 septembre 2013 à http://www.computerweekly.com/feature/How-to-tackle-big-data-from-a-security-point-of-view.

[43] Deibert, Ron. *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in cyberespace*. Préparé pour le Canadian Defence & Foreign Affairs Institute. Août 2012.

[44] Voir par exemple, Symantec « New Survey Shows U.S. Small Business Owners Not Concerned About Cybersecurity; Majority Have No Policies or Contingency Plans » (octobre 2012); « Canadian businesses unprepared for cyber attacks: Queen's University expert » (mai 2013); Computerworld.au « Companies still unprepared for cyber attacks: Deloitte » (février 2013); CBC « Canadian companies open to cyber attacks, says federal agency » (juillet 2013).

[45] Cela figure dans plusieurs sources, notamment : Deibert, Ron. *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in cyberespace;* Misha Glenny « Canada's weakling Web defences », *Globe and Mail*, 18 mai 2011; Rapport d'automne du Bureau du vérificateur général (2012), Chapitre 3 — Protéger l'infrastructure canadienne essentielle contre les cybermenaces; Alexandra Posadzki « Cyber security in private sector a 'significant' problem: Public Safety records », la Presse canadienne, 14 juillet 2013. Matthew Braga « Canada must ramp up cyber security in wake of alleged China-led attacks, experts say », *Financial Post,* 19 février 2013.

[46] « Study of the Impact of Cyber Crime on Businesses in Canada ». *International Cyber Security Protection Alliance* (mai 2013).

[47] Ibid.

[48] Ibid.

[49] *Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée*. Préparé pour le Commissariat à la protection de la vie privée du Canada par Phoenix Strategic Perspectives Inc. 2013.

[50] Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée. Préparé pour le Commissariat à la protection de la vie privée du Canada par Phoenix Strategic Perspectives Inc. 2014.

[51] Info Security « Gartner Says Risk-Based Approach will Solve the Compliance vs Security Issue », publié le 8 août 2013.

[52] Ibid.

[53] Ibid.

[54] Deibert, Ron. « Canada and the Challenges of cyberespace Governance ». University of Calgary School of Public Policy (SPP) Communiqué. Vol. 5, numéro 3, mars 2013.

[55] « *Canada and Cyberespace: Key Issues and Challenges* » (2012). Rapport préparé par SecDev Group, commandé par le ministère des Affaires étrangères, du Commerce et du Développement (MAECD).

[56] See Deibert, Ron. « Canada and the Challenges of cyberespace Governance ». University of Calgary School of Public Policy (SPP) Communiqué. Vol. 5, numéro 3, mars 2013.

[57] Concepts de Deibert, R. et Rohozinski, R. « Risking Security: Policies and Paradoxes of cyberespace Security », *International Political Sociology* (2010), propos cités par Deibert, Ron. *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in cyberespace*. Août 2012, et Deibert, Ronald J. (2013) *Black Code: Inside the Battle for cyberespace*. McClelland & Stewart.

[58] Dupont, Benoit « The proliferation of cyber security strategies and their implications for privacy. » *Circulation internationale de l'information et sécurité.* Karim Benyekhlef et Esther Mijans (eds.) Les Éditions Thémis. Pages 67-80-2013. Consulté en ligne le 17 juin 2013 à http://www.benoitdupont.net/node/145.

[59] Deibert, R. et Rohozinski, R. « Risking Security: Policies and Paradoxes of cyberespace Security ». *International Political Sociology* (2010), propos cités par Deibert, Ron. *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in cyberespace*. Août 2012.

[60] Deibert, Ronald J. (2013) *Black Code: Inside the Battle for Cyberspace*. McClelland & Stewart.

[61] Ibid.

[62] Ibid.

[63] Ibid.

[64] ISO/IEC 27032:2012(E) Information Technology – Security Techniques – Guidelines for Cybersecurity (published 16 July 2012) http://webstore.iec.ch/preview/info_isoiec27032%7Bed1.0%7Den.pdf

[65] Deibert, Ronald J. (2013). *Black Code: Inside the Battle for cyberespace*. McClelland & Stewart.

[66] Deibert, Ron. *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in cyberespace*. Préparé pour le Canadian Defence & Foreign Affairs Institute. Août 2012.

[67] *Plan d'action 2010-2015 de la Stratégie de cybersécurité du Canada* (le Plan d'action). Lancé en avril 2013.

[68] Voir la page 35 de « *Canada and Cyberespace: Key Issues and Challenges* » (2012). Rapport préparé par SecDev Group, commandé par le ministère des Affaires étrangères, du Commerce et du Développement (MAECD). Les fournisseurs aux États-Unis, au Canada et en Europe sont les principaux producteurs d'outils qui rendent possible l'inspection approfondie des paquets d'information, le filtrage des contenus, l'exploration des réseaux sociaux, le suivi des téléphones cellulaires et les attaques de réseaux informatiques.

[69] Voir page 6 de « *Canada and Cyberespace: Key Issues and Challenges* » (2012). Rapport préparé par SecDev Group, commandé par le ministère des Affaires étrangères, du Commerce et du Développement (MAECD).

[70] Allocution de Chantal Bernier, « Nouvelles plateformes, nouvelles mesures de protection : protéger la vie privée dans le cyberespace. » Remarques dans le cadre de la Conférence donnée au Centre de la sécurité nationale et organisée par le Conference Board du Canada.

[71] Opinion du CEPD. Avis du Contrôleur européen de la protection des données sur la communication conjointe de la Commission et de la Haute Représentante de l'Union pour les affaires étrangères et la politique de sécurité sur: 'Cyber Security Strategy of the European Union : an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union *(Ce document n'est pas actuellement disponible dans toutes les langues)*. Bruxelles, 17 juin 2013.

[72] EUROPA Communiqué de presse : « Respect de la vie privée et confiance doivent être les fondements de toute stratégie de cybersécurité crédible en Europe. » 17 juin 2013. http://europa.eu/rapid/press-release_EDPS-13-6_fr.htm?locale=en.

[73] Allocution de Chantal Bernier, « Discussion sur l'équilibre entre la protection des renseignements personnels et l'application de la loi. » Remarques dans le cadre d'une conférence intitulée « Securing the Cyber Commons: A Global Dialogue », organisée par le Canada Centre for Global Security Studies, la Munk School of Global Affairs, l'University de Toronto et le groupe SecDev. (28 mars 2011).

[74] Ministère des Affaires étrangères, du Commerce et du Développement – Rapport sur les plans et les priorités de 2013-2014, disponible à http://www.international.gc.ca/department-ministere/assets/pdfs/RPP_2013_2014_FRA.pdf.

[75] Aussi connu sous le nom de Convention de Budapest, ce document est le seul instrument international juridiquement contraignant conçu expressément pour lutter contre la cybercriminalité. La Convention de Budapest sert de lignes directrices pour tout pays élaborant une législation exhaustive en matière de cybercriminalité, mais aussi de cadre pour la coopération internationale contre la cybercriminalité parmi les États Parties. On peut consulter le document à http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_fr.asp.

[76] Voir le site Web de la *Loi canadienne anti-pourriel* http://laws-lois.justice.gc.ca/fra/lois/E-1.6/index.html.