Rapport évolutif

Analyse des impacts de la mondialisation sur la sécurité au Québec

Rapport 5 — De la cybercriminalité au déploiement de la cybersécurité

Laboratoire d'étude
sur les politiques publiques
et la mondialisation

Monica Tremblay, M. Sc.
Anthropologue

Décembre 2007

École nationale
d'administration
publique

INTRODUCTION

Instruments de la mondialisation, les technologies de l'information et Internet sont venues simplifier les communications sur la planète. En 2007, peu de personnes et d'organisations échappent à l'utilisation des systèmes informatiques. Un citoyen, une entreprise, un gouvernement et ses différentes organisations, tous sont des acteurs qui, d'une part, peuvent utiliser des systèmes informatiques et manipuler des informations et, d'autre part, souhaitent les protéger pour différentes motivations.

La sécurité des États, de leurs entreprises et de leurs citoyens est affectée par les nouvelles menaces qui proviennent du cyberespace. Avec le réseau Internet qui ouvre la porte sur le monde, des menaces propres à l'univers informatique sont apparues : virus informatiques, vers, hameçonnage, etc. Quant aux menaces dites traditionnelles : vol d'identité, trafic d'armes, blanchiment d'argent, et autres, l'utilisation d'Internet en a décuplé l'impact. L'Internet rend les organisations, quelle que soit leur envergure, vulnérables à diverses formes d'incidents qui transcendent les frontières. Parfois, ces incidents n'ont pas de répercussions majeures, dans d'autres cas, les impacts sont énormes.

Au chapitre des nouvelles menaces, les journaux ont fait état, au cours des derniers mois, de différentes cyberattaques. Ces dernières ont été perpétrées envers les systèmes informatiques de quelques États, notamment l'Estonie, les États-Unis, la Nouvelle Zélande, la France et l'Allemagne. Les journaux rapportent aussi des fuites de données des systèmes informatiques d'entreprises multinationales. Que signifie cela? Les États et les entreprises sont-ils préparés à ces types de menace? Qu'en est-il du Québec? Est-il à l'abri d'une cyberattaque? Doit-il se préoccuper de sécurité informatique? Si tel est le cas qui devrait alors s'en préoccuper? Par quels moyens les États se protègent-ils et protègent-ils les citoyens et les entreprises? Ce sont là des questions auxquelles ce rapport souhaite apporter un éclairage.

Ce rapport porte principalement sur des démarches de sécurité informatiques de nature politique, légale et administrative plutôt que de nature technologique. Il expose différentes démarches gouvernementales d'ici et d'ailleurs, ainsi que des démarches du privé visant à réduire les risques liés à la cybercriminalité.

Pour commencer, quelques notions sont clarifiées. Par la suite, un regard est posé sur des actions entreprises, sur le plan international, au Canada et au Québec, afin de se prémunir contre les crimes informatiques que peuvent subir les États et qui peuvent avoir des répercussions sur les citoyens et les entreprises. Pour terminer, deux exemples concrets de systèmes informatiques québécois pour lesquels la sécurité est une préoccupation sont présentés. Enfin, en conclusion, certains enjeux et quelques questions sont soulevées.

1. SÉCURITÉ INFORMATIQUE ET CYBERCRIMINALITÉ

Parler de sécurité informatique conduit à évoquer les risques de cybercriminalité. On ne peut pas discuter de sécurité informatique sans identifier ce qu'il faut sécuriser, contre quoi et contre qui. Il faut regarder le contexte dans lequel la sécurité informatique doit être déployée. Ainsi, les risques s'inscrivent dans un contexte culturel, organisationnel, historique, politique et technologique donné. Par exemple, outre l'Internet, les événements du 11 septembre 2001 teintent ce contexte sous l'angle socio-historique et politique. Comme dans le monde matériel, les risques relatifs au cyberespace peuvent être causés par des accidents, par des

erreurs ou par de la malveillance. Que les menaces soient intentionnelles ou non, la sécurité informatique vise généralement à se prémunir contre tout incident qui pourrait perturber le fonctionnement normal des systèmes informatiques desquels dépendent de plus en plus les organisations et les États.

La **sécurité informatique**, selon le dictionnaire terminologique de l'Office québécois de la langue française, est défini comme un «ensemble de mesures de sécurité physiques, logiques et administratives, et de mesures d'urgence, mises en place dans une organisation, en vue d'assurer la protection de ses biens informatiques, la confidentialité des données de son système d'information et la continuité de service» (OQLF, sept. 2007). Ainsi, la sécurité informatique a pour objectif d'assurer pour tous les acteurs concernés (gouvernements, entreprises et citoyens) l'intégrité, la confidentialité, l'irrévocabilité, la disponibilité et la fiabilité, l'authentification ainsi que la qualité des informations et de la technologie (OQLF, 2007; Ghernanouti-Hélie, 2006, 2002; Pillou 2005; Filiol et Richard, 2006).

Les types de cybercriminalité sont nombreux. Toutefois, ce rapport se penche sur les crimes que peut subir un État et qui peuvent avoir des répercussions sur les citoyens et les entreprises. Il sera fait abstraction des méfaits tels que la pornographie infantile sur Internet. Les crimes qui concernent les informations sensibles, comme les renseignements personnels, les renseignements économiques ou financiers et stratégiques, sont au cœur de ce rapport.

Le vocabulaire qui circule présentement peut prêter à confusion. Malgré l'existence de liens entre les termes, il ne s'agit pas de synonymes. C'est pourquoi, des précisions sur la cybercriminalité, les cyberattaques, le cyberterrorisme et la cyberguerre sont présentées ci-après.

D'abord, la **cybercriminalité** peut être définie comme «tout crime ou délit dans lequel l'ordinateur est soit le moyen, soit le but.» (Filiol et Richard, 2006 : 2). Ainsi la cybercriminalité englobe toutes les infractions possibles pouvant être commises à l'aide d'Internet et envers Internet. Il y a bien entendu les délits «conventionnels»[1] tels que le détournement de fonds, la distribution de pornographie juvénile, le télémarketing frauduleux, la fraude, la vente de biens volés et illégaux, le vol de propriété intellectuelle, etc. S'ajoutent à ces derniers les délits «innovateurs»[2], c'est-à-dire les infractions qui n'existaient pas avant le développement de l'informatique et d'Internet parce qu'ils peuvent uniquement être réalisés dans l'univers virtuel, comme obtenir frauduleusement des services d'ordinateur, intercepter illégalement une fonction d'ordinateur, posséder ou utiliser un mot de passe pour l'utilisation non autorisée d'ordinateur ou encore pour accéder à une base de donnée ou surcharger un système informatique afin d'empêcher une organisation d'offrir ses services adéquatement. Bref, la cybercriminalité inclut les «actes, portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des données et des systèmes informatiques» (Conseil de l'Europe, 2001).

Une autre caractéristique de la cybercriminalité est étroitement liée à l'ouverture sur le monde que procure Internet. La cybercriminalité a pour force d'être rapide, efficace et sans frontières. Elle se déroule dans le cyberespace qui, grâce à son étendue, permet aux auteurs de crimes de conserver un anonymat relatif. Il apparaît dès lors plus difficile dans ce contexte d'arrêter les criminels puisqu'ils peuvent se cacher n'importe où dans le monde.

Le terme **cyberattaque** est quant à lui utilisé pour désigner un cybercrime qui a effectivement été perpétré. Par exemple, on parlera de cyberattaques, et plus particulièrement de déni de service[3] lorsque les sites gouvernementaux ou autres sites sont bombardés en multipliant de façon faramineuse le nombre de visite par seconde. Ces attaques font partie de la méthode qualifiée d'intrusion logique. Il existe bien d'autres méthodes d'attaques. Panko (2004) précise qu'il peut y avoir des attaques par accès physique (intrusion sur un serveur), des attaques par dialogue (usurpation d'identité), des attaques par intrusion logique (virus) et des attaques qualifiées d'ingénierie sociale (vol d'informations, vol de mots de passe).

Le **cyberterrorisme**, peut être défini comme une forme de terrorisme (classique) où les finalités demeurent les mêmes mais où les moyens changent. Il s'agit d'«une action violente et symbolique ayant pour mandat de faire changer des comportements sociopolitiques en dérangeant les opérations normales de la société. Avec le cyberterrorisme, les attaques visent les réseaux informatiques importants qui constituent un des piliers des sociétés technologiquement évoluées» (Gagnon, B. 2002 : A15). Par exemple, une attaque pourrait viser des infrastructures stratégiques d'un État telles que les infrastructures énergétiques, les réservoirs d'eau, les télécommunications et les banques, entraînant de graves répercussions pour la société (Ghernaouti-Hélie, 2006) [4].

Enfin, la **cyberguerre** concerne d'avantage les forces armées et fait référence à l'utilisation des technologies de l'information et des communications (TIC) et à l'informatique dans l'organisation militaire. Néanmoins, il est possible que des répercussions se fassent sentir chez les civils et que les conséquences soient désastreuses sur le terrain. La cyberguerre viserait à «perturber autant que possible le fonctionnement des opérations militaires – tout ce qui peut contribuer à diminuer la capacité à se défendre» (Dunnigan in Terrorrisme.net, 2002).

2. RISQUES DE CYBERATTAQUES ET IMPACTS À CONSIDÉRER

L'avènement d'Internet a permis le développement du commerce électronique et du gouvernement en ligne. Or, cette offre de services électroniques, publics ou privés, a accru les risques informatiques qui peuvent affecter les gouvernements, les entreprises et les citoyens. De plus en plus, les journaux rapportent des cyberattaques commises envers des gouvernements. Selon Chandler (2004), auteure d'un article sur la sécurité dans le cyberespace, les cyberattaques continueront d'augmenter. D'ailleurs, des publications spécialisées font état de tentatives et d'attaques informatiques plus fréquentes et plus nombreuses, notamment aux États-Unis, que celles qui sont rapportées dans les médias de masse. Les organisations publiques et privées ont tendance à cacher à leurs clientèles les attaques informatiques dont elles sont victimes par peur de générer de l'insécurité et une perte de confiance dans leurs systèmes.

Quels sont donc les risques et les menaces contre lesquels doivent se protéger les différents acteurs? Dans bien des cas, les crimes traditionnels ont été transposés dans l'espace virtuel. À cette réalité se sont additionnés les crimes directement liés à l'utilisation des TIC, et plus particulièrement de l'Internet. Les crimes perpétrés viennent bousculer les préoccupations de la société. Actuellement la tendance est, entre autres, à la recherche de transparence de la part des dirigeants, d'efficience des services publics, de sécurité du territoire, ainsi que de respect de vie privée et d'autonomie

des citoyens. Les crimes peuvent perturber le bon fonctionnement d'un État, d'un gouvernement, d'une entreprise. Ils peuvent aussi avoir des répercussions sur les services à rendre aux citoyens, que ce soit pour assurer leur sécurité ou pour leur offrir d'autres services essentiels. Un citoyen voudra être certain que les informations que détient l'État à son sujet ne seront pas modifiées, altérées ou divulguées à de tierces parties sans qu'il en ait été informé[5]. Citoyens, entreprises et gouvernements souhaitent aussi que les infrastructures stratégiques (énergie, eau, santé, transport…) ne soient pas affectées par une quelconque menace. Pensons seulement aux installations énergétiques. Une perturbation du réseau électrique affecterait par ricochet le fonctionnement des autres infrastructures stratégiques de la société, ce qui aurait des répercussions sur l'économie et la sécurité nationale. C'est pour cette raison qu'une des priorités du Québec, formulée dans La Politique internationale du Québec (MRI, 2006a : 77) consiste à renforcer la sécurité des infrastructures stratégiques. L'exemple de la ville de Montréal est aussi évocateur. Cette dernière annonçait récemment des travaux visant à sécuriser ses réservoirs d'eau contre différents dangers, dont les menaces terroristes (Baillargeon, 2007). Le gouvernement du Canada affichait, il y a quelques années, une préoccupation similaire.

« La sécurité informatique constitue le principal défi transfrontalier auquel font face les infrastructures essentielles du Canada, le gouvernement fédéral renforcera sa capacité de prévoir et de contrer d'éventuelles cyberattaques. On est en train de créer un groupe de travail national de haut niveau, composé de représentants des secteurs public et privé, en vue d'élaborer une stratégie nationale de cybersécurité. (Sécurité publique Canada, 2004) »

Compte tenu des impacts négatifs qu'entraine une cyberattaque, il apparaît important de se préoccuper de la sécurité informatique (Chandler 2004). Les attaques entraînent des coûts d'ordre divers pour les organisations affectées. Par exemple, une attaque, telle que le déni de service, peut occasionner de sérieux dommages à une organisation et aux acteurs qui sont en relation avec elle. Cela peut entraîner, notamment, des coûts matériels et financiers, entacher l'image de l'organisation, susciter la perte de confiance en un gouvernement ou, dans les moyens de communiquer avec lui. Dans le cas de l'Estonie, plusieurs institutions (écoles, journaux, banques…) ont été perturbées dans leur travail. La situation a également requis l'intervention de l'OTAN à des fins d'enquête. Parmi les retombées négatives possibles on constate, dans ce cas, la possibilité de détérioration des relations avec un autre État, celui d'où semble provenir l'attaque. Il faut toutefois éviter de sauter aux conclusions. Il n'a pas été confirmé que ces attaques constituent un acte de cyberguerre. La preuve doit d'abord être faite puisque les criminels pourraient seulement avoir «emprunté» de façon illicite les réseaux d'ordinateurs à l'insu des personnes ou des organisations qui les possèdent. Par exemple, la Chine, récemment accusée par d'autres États, affirme être elle-même victime d'infiltration informatique et de subversion (Olanié, 2007). Un autre exemple récent, cette fois dans le secteur privé, illustre comment peut être entachée l'image d'une entreprise. L'entreprise TJX Companies qui a été victime d'un vol de renseignements personnels sur plusieurs de ses clients devra travailler ferme à rétablir la confiance auprès de l'ensemble de ses clients (Commissariat à la protection de la vie privée du Canada, 2007)[6].

Au Québec, les ministères et organismes «recueillent, conservent, utilisent et diffusent de plus en plus de données sous forme

numérique, et en grande quantité. Parfois de nature personnelle ou confidentielle, ces données peuvent avoir une valeur juridique, administrative, économique ou patrimoniale» (MSG, 2007a). D'où l'importance qu'accorde le Québec à la protection des infrastructures stratégiques telles que les systèmes d'information et les bases de données.

3. CYBERCRIMINALITÉ, SÉCURITÉ INFORMATIQUE ET ACTIONS PRÉVENTIVES

Afin de se prémunir face à la cybercriminalité, différentes actions d'ordre international, national et local sont réalisées. De façon générale, les actions visant à instaurer la sécurité informatique peuvent être qualifiées de préventives (Ghernaoui-Héli, 2000). Au nombre des actions préventives se trouvent, entre autres, la création d'organisations ou de comités spéciaux, le développement de services informatiques particuliers visant à assurer la sécurité ainsi que les actions de sensibilisation et de formation. Le développement et l'ajustement du cadre légal font également partie des actions préventives. La plupart des États ont de nombreuses lois, politiques et directives qui concourent à encadrer la cybercriminalité et à assurer la sécurité informatique. Compte tenu de la nature transfrontalière de la cybercriminalité, il est apparu nécessaire de favoriser la coopération entre les États afin de prévenir les cybercrimes. Parmi les stratégies de prévention internationales, il ressort la nécessité des pays à s'entendre mutuellement sur les moyens de sanctionner les cybercrimes. En condamnant les auteurs des cybercrimes, on vise à dissuader la récidive et les cybercriminels potentiels.

Certaines initiatives internationales concernant la sécurité informatique méritent d'être mentionnées. Elles permettent de mieux comprendre le contexte mondial dans lequel s'inscrivent les initiatives du Québec. Face à la cybercriminalité, les États ont dû revoir leurs lois ou en adopter de nouvelles afin de pouvoir juger et réprimer les actes malveillants.

3.1 Initiatives internationales

En 1992, quelques années après l'explosion de l'utilisation d'Internet, l'**OCDE** a formulé des lignes directrices concernant la sécurité des systèmes d'information. Dix ans plus tard, en 2002, elle a revu ces lignes directrices afin d'y intégrer la sécurité des réseaux d'information. Ces lignes directrices émises par l'OCDE ont pour objectif de favoriser le développement d'une culture de la sécurité.

Le **G8** a pour sa part mis en place en 1997 le *G8's Subgroup of High-Tech Crime*. Ce comité a depuis adopté 10 principes de lutte aux crimes informatiques. Ces principes encouragent une approche unifiée entre les États afin d'améliorer la lutte à la cybercriminalité. À l'aide de ces principes, le G8 souhaite éviter les possibles brèches dans les mesures législatives des États qui permettraient aux contrevenants d'être à l'abri des poursuites. Le premier principe stipule notamment qu' «il ne doit pas y avoir de 'paradis de sécurité' pour ceux qui abusent des technologies de l'information» [Notre trad.] (G8, 1997 : 3).

Dans cette même lignée, l'**ONU** a émis en 2000 une recommandation[7] visant à lutter contre l'utilisation criminelle des technologies de l'information (TI). Elle suggère que les États s'assurent que leurs lois et pratiques ne contiennent pas de failles qui permettraient aux auteurs de crimes de ne pas être pénalisés. De plus, il est recommandé que le système légal couvre, les systèmes informatiques (confidentialité, intégrité et disponibilité) et qu'il punisse les crimes ou les abus.

Une autre initiative internationale de plus grande envergure est la *Convention sur la cybercriminalité*. Elle a été adoptée en 2001 par le **Conseil de l'Europe**. Cette convention a été élaborée par 43 pays. Parmi ceux-ci figuraient des États membres du Conseil de l'Europe ainsi que 4 autres États non membres : les États-Unis, le Canada, l'Afrique du Sud et le Japon. En février 2007, 21 pays avaient ratifié cette convention. Il serait intéressant de voir pourquoi près de la moitié des pays à l'origine de sa création tardent ou refusent de la ratifier. Parmi les États non membres, seul les États-Unis l'ont ratifiée jusqu'ici. Elle y est d'ailleurs en vigueur depuis janvier 2007.

Cette convention est née du besoin d'avoir une politique pénale internationale commune destinée à protéger la société des crimes commis dans le cyberespace. Son champ d'application s'étend à la plus grande partie du trafic informatique mondial. Elle cherche d'abord à harmoniser les législations nationales quant à la définition des crimes. Elle espère ensuite établir les moyens d'enquête et les moyens de poursuites pénales de sorte qu'ils soient «adaptés à la mondialisation des réseaux». Enfin, la Convention espère mettre en place «un système rapide et efficace de coopération internationale». Ainsi, elle «prévoit des règles de base qui devraient faciliter la conduite d'enquêtes dans le monde virtuel et qui représentent de nouvelles formes d'entraide judiciaire.» (Conseil de l'Europe, nov. 2001).

Concernant l'entraide, la Convention prévoit un réseau disponible 24 heures sur 24, sept jours sur sept, afin d'assurer une assistance immédiate en cas d'infractions criminelles contre des systèmes informatiques.

« En ratifiant ou adhérant à la Convention sur la cybercriminalité du Conseil de l'Europe, ou en mettant en œuvre ses principes, les États consentent à s'assurer que leurs lois internes criminalisent des conduites décrites dans la section principale de droit criminel et établissent les outils procéduraux nécessaires afin d'examiner et de poursuivre de tels crimes. Il s'agit là de l'approche nationale légale sur le cybercrime [Notre trad.] (Scholberg 2006).»

L'**Union Européenne** en 2002 a proposé un Cadre décisionnel concernant les attaques des systèmes d'information. Ce cadre, adopté en 2005, vise à réprimer et punir les actes criminels tels que l'accès illégal aux informations, l'interférence des systèmes d'information et l'altération des données.

Le **Commonwealth** a adopté, en se basant sur la Convention sur la cybercriminalité, un modèle de loi, Model Law on Computer and Computer Related Crime, afin de favoriser la compatibilité des lois relatives à l'informatique entre les États du Commonwealth (Commonwealth, 2002).

L'**Organisation des États d'Amérique** (OEA) a créé un groupe d'experts sur le cybercrime. Celui-ci a engagé différentes activités visant à favoriser la coopération internationale de lutte à la cybercriminalité. Ce groupe a notamment organisé une conférence en 2005 sur la «responsabilité globale» face au défi que représente le cybercrime. De plus, l'OEA encourage fortement la coopération des États membres avec le Conseil de l'Europe. Elle suggère l'adhésion à la Convention sur la cybercriminalité afin que soient instaurés des lois et d'autres instruments qui permettent de lutter efficacement contre la cybercriminalité autant au niveau local qu'international. L'OEA encourage également le renforcement des mécanismes d'échange d'information et de coopération avec les autres organisations internationales qui luttent contre la cybercriminalité.

Du côté de l'Asie, des démarches de coopération pour la lutte à la cybercriminalité ont aussi été lancées. Ainsi, l'**Asia Pacific**

Economic Cooperation a créé le *e-security Task Group*. **L'Association of Southeast Asian Nations** a, quant à elle, signée avec la Chine une entente visant à maintenir et à améliorer la cybersécurité ainsi que la prévention et la lutte à la cybercriminalité. Cette association a elle aussi reconnu l'importance de favoriser la coopération internationale en matière de législation de lutte à la cybercriminalité. Cette position a été prise lors d'une réunion ministérielle sur le crime transnational en 2004.

Outre les organisations internationales étatiques, il existe des organisations internationales privées qui veillent à promouvoir la sécurité informatique. Ces entreprises réalisent des veilles et des analyses des nouvelles menaces informatiques et les communiquent à leurs clients[8]. Des organisations de différents États proposent également des services de veilles à la communauté internationale à propos des menaces existantes.

Plusieurs États, inspirés par les États-Unis, se sont doté d'équipes de réaction aux incidents, les Computer Emergency Response Team (CERT)[9]. Un CERT étudie les problèmes informatiques et les réseaux de sécurité. Cela lui permet d'être prêt à intervenir en cas de cyberattaques. Il sensibilise aussi les utilisateurs à propos des menaces et aide à améliorer la sécurité informatique. En Europe, 110 CERT ont récemment été recensés (Hakkaja, 2007). Au Canada, le Centre canadien de réponse aux incidents cybernétiques (CCRIC) joue le rôle d'un CERT. Il est «chargé de la surveillance des menaces et de la coordination des interventions aux incidents de sécurité cybernétique» (Sécurité publique Canada. 2007). Le Québec a aussi créé le CERT/AQ, CERT de l'administration québécoise, pour exercer ce rôle de gestion d'incidents de sécurité informatique.

D'autres types d'initiatives qui rallient plusieurs pays ont été instaurées aux fins de sécurité. C'est le cas du projet Échelon dirigé par l'Agence nationale de sécurité (NSA) des États-Unis. Échelon est un système automatisé d'interception mondiale des échanges électroniques. Ce système est exploité par les services de renseignements des États-Unis, du Canada, de l'Australie, du Royaume-Uni et de la Nouvelle-Zélande (Schneier 2000). De façon générale, concernant la sécurité informatique, les États s'inspirent de l'expérience des autres. Toutefois, il faut souligner que les États-Unis, suite aux événements de septembre 2001, ont tracé, en matière administrative et légale, une voie que la communauté internationale a tendance à suivre. De plus, les États-Unis ont «la part plus facile : maître du réseau Internet, distributeur monopolistique de systèmes d'exploitation et de processeurs, artisan de la plupart des normes, une infrastructure mondiale d'espionnage comme Échelon… bref les États-Unis ont tous les moyens d'agir à leur guise.» (Filiol et Richard 2006 :180-181). Il faut aussi préciser que, depuis le 11 septembre, les États-Unis obligent plusieurs autres pays à resserrer leurs mesures de sécurité nationale, notamment par l'exigence d'un passeport biométrique.

3.2 Initiatives canadiennes

Le Canada est un des chefs de file en matière d'utilisation des technologies de l'information dans l'offre de services publics, notamment, depuis la mise en place du gouvernement en ligne. Dans ce contexte, plusieurs lois et politiques ont été adoptés ou bonifiés afin de prévenir et sanctionner les méfaits liés à l'informatique non seulement ceux perpétrés dans le secteur public, mais aussi ceux du secteur privé. Le Canada a, entre autres, adopté des amendements au Code criminel, amendements qui ont permis d'y inclure les cybercrimes.

Le Canada dispose de plusieurs lois et politiques à prendre en considération lorsqu'il est question de sécurité informatique[10]. Au Canada, les organisations gouvernementales doivent se conformer, à tout le moins, à une vingtaine de lois, politiques et directives. Chacune de ces lois et politiques a pour objectif de protéger les données, la confidentialité et la disponibilité des informations. À cela s'ajoutent les directives internationales que les États sont fortement encouragés à mettre en œuvre et à respecter.

En 2007, le Canada a adopté une *Politique sur la gestion de l'information* en remplacement de deux autres politiques. Cette politique vise à «préserver l'information et veiller à l'accès à l'information et aux documents […] » (SCT Canada, 2006).

« La gestion et la diffusion de l'information font partie intégrante de l'exécution des programmes et de la prestation des services, et ces fonctions sont présentes dans tous les aspects de la législation et elles y sont assujetties. Les exigences en matière de gestion de l'information sont implicites dans le cadre global des lois canadiennes et elles sont explicitement définies dans les lois et les politiques qui ont trait, en tout ou en partie, aux directives du gouvernement en ce qui a trait à la gestion de l'information. (SCT Canada, 2006 : 5).»

Par ailleurs, le Canada est membre de quelques organisations internationales et comités spéciaux de lutte à la cybercriminalité transnationale. Il a notamment participé à la préparation de la Convention sur la cybercriminalité. Il fait partie du groupe de travail de l'OEA et des groupes d'experts du G8 contre le terrorisme (Groupe de Rome) et contre la criminalité (Groupe de Lyon). Le Canada participe aussi à un partenariat intégré entre les organismes internationaux, fédéraux et provinciaux d'application de la loi, dans le cadre du Centre de Signalement en direct des délits économiques (Centre RECOL)[11].

De plus, afin de lutter contre la cybercriminalité, la Gendarmerie Royale du Canada (GRC) a développé des partenariats avec les organisations internationales, fédérales et provinciales. À ce propos, la GRC a créé un site web concernant la criminalité informatique.

Parmi les stratégies de lutte à la cybercriminalité, le Canada compte sur une banque de données pour les services de renseignements criminels : *Le Système automatisé de renseignements sur la criminalité (SARC)*. Ce système pancanadien est géré par le bureau central du Service canadien de renseignements criminels (SCRC).

Conscient de l'importance de la sensibilisation, le Canada a fait d'octobre 2007 le «Mois de la sensibilisation à la cybersécurité». Par cette action, le gouvernement souhaite sensibiliser la population aux risques de l'utilisation de l'Internet et encourager celle-ci « à adopter des mesures de sécurité cybernétiques ». (Sécurité publique Canada, 2007). Cet événement est l'occasion d'offrir des informations sur les outils et les moyens disponibles qui permettent d'utiliser les systèmes informatiques d'une manière sécuritaire. Cela permet aussi de reconnaître les efforts menés par le secteur privé pour sécuriser les activités sur Internet. Le Canada joint indirectement ses efforts de sensibilisation à ceux des États-Unis pour qui octobre est également le mois de la prévention de la cybersécurité nationale. Selon Filiol et Richard (2006 : 169), certains États, notamment les pays anglo-saxons, investissent davantage de ressources humaines et financières dans la «sensibilisation des victimes potentielles» qu'il s'agisse d'individus ou d'entreprises privées ou publiques.

3.3 Initiatives québécoises

En tant qu'État qui possède et utilise d'importantes infrastructures informatiques, le Québec ne peut pas négliger les risques associés à la cybercriminalité. D'ailleurs, la sécurité informatique fait partie des priorités de la *Politique internationale du Québec* (MRI, 2006a : 77). Afin de concrétiser cette priorité, la collaboration avec d'autres États «sur la sécurisation des systèmes informatiques publics et la protection des renseignements personnels» fait partie du scénario. (MRI, 2006b: 2; MRI, 2006a). Déjà, pour se prémunir contre différentes menaces, le gouvernement du Québec favorise la collaboration avec d'autres États et participe au développement de la sécurité à l'échelle internationale. Pour ce faire, il mise sur «le partage d'informations, d'expertises et de façons de faire. Il participe au développement de pratiques innovatrices et de nouvelles technologies dans le but d'améliorer la sécurité» (Gouvernement du Québec, 2006: 2). Il a d'ailleurs signé des accords et des ententes de sécurité avec des gouvernements, des villes et des organismes publics, principalement avec des États américains limitrophes (Ranger, 2004)[12]. Le Québec a aussi une entente d'entraide mutuelle avec les provinces de l'Atlantique et certains États limitrophes états-uniens afin d'assurer une meilleure protection de la population en cas d'urgence. La possibilité d'une catastrophe technologique fait partie de ces urgences.

La participation du Québec au *Council of State Governments*, dont il est membre affilié depuis 1995, constitue un autre exemple de l'implication internationale québécoise. Pour le Québec, il s'agit d'une implication stratégique puisque de nombreux dossiers traités au sein de ce conseil concernent les questions transfrontalières, notamment la sécurité publique et le secteur de l'énergie (Assemblée nationale).

Le souci d'une collaboration internationale du gouvernement du Québec transparaît également dans des actions internes. C'est notamment le cas lorsqu'il travaille au renforcement de la vérification des documents d'identité qu'il émet afin de tenir compte de l'évolution des nouvelles normes nord-américaines. En outre, compte tenu de son statut d'État fédéré, le Québec doit tenir compte des lois fédérales telle que la *Loi sur la protection des renseignements personnels et les documents électroniques.*

Depuis quelques années déjà, parallèlement à l'utilisation des nouvelles technologies de l'information et des communications (NTIC) et ensuite à l'implantation du gouvernement en ligne, le Québec a commencé à se doter de différentes lois et d'autres documents administratifs permettant de mieux refléter la réalité du monde numérique. Le développement de ces lois et d'autres dispositions poursuit l'objectif, d'une part, de faciliter et d'harmoniser, voir normaliser, l'utilisation des technologies de l'information et, d'autre part, de conférer aux informations électroniques la même valeur juridique que les documents matériels dans la mesure où les documents électroniques sont protégés par des mesures d'intégrité suffisantes. Ces principes se retrouvent notamment dans la Loi concernant le cadre juridique des technologies de l'information. Le gouvernement du Québec a aussi adopté la *Politique québécoise de l'autoroute de l'information* en 1998 afin de mettre en évidence l'importance pour le gouvernement de bâtir un environnement électronique sécuritaire. Elle a aussi permis de «mettre en place un ensemble de mesures de nature technologique, administrative et juridique susceptibles d'instaurer et d'entretenir un climat de confiance dans les échanges électroniques.»(MSG, 2007b).

Afin d'instaurer la confiance, le gouvernement s'est aussi préoccupé de la gestion de la sécurité de l'information. Pour ce faire, il a élaboré la Directive sur la sécurité de l'information gouvernementale, en vigueur depuis le 1er mai 2006.

« La Directive sur la sécurité de l'information gouvernementale a pour objet d'établir une vision commune de la sécurité de l'information gouvernementale et d'assurer la cohérence et la coordination des interventions en cette matière. Elle repose sur une approche globale et une gestion intégrée des aspects humains, juridiques, organisationnels, techniques et d'éthique requis pour assurer la sécurité de cette information. (MSG, 2007b) »

Ainsi, tout comme la nécessité d'accorder les lois entre les États, une harmonisation du cadre légal auquel sont soumises les organisations d'un même ordre de gouvernement est nécessaire. Au Québec, les lois et politiques à respecter pour assurer la sécurité informatique sont nombreuses et répondent à des préoccupations spécifiques. Par exemple, elles encadrent l'accès à l'information, la conservation des données, ou encore l'utilisation éthique du courriel[13]. D'autres lois et politiques, qui ne se rapportent pas spécifiquement à la sécurité informatique, doivent tout de même être considérées. Plusieurs comprennent des clauses qui visent à protéger les renseignements détenus dans les systèmes informatiques. C'est le cas, notamment, des lois sectorielles, telle que la Loi sur la RAMQ ou la Loi du MRQ. En plus, les organisations ont la responsabilité de définir leur politique interne de sécurité[14]. Une visite des sites des ministères du gouvernement du Québec permet de constater que les ministères qui offrent des services en ligne et qui requièrent des informations et des données personnelles, rendent publique les mesures de sécurité en vigueur sur leur site. En particulier, les ministères affichent sur leur site leur politique de confidentialité qui informe l'usager à propos de la sécurité des échanges d'informations qu'il peut avoir avec le ministère.

Le gouvernement du Québec a aussi constitué un réseau d'alerte des responsables en sécurité informatique. Les responsables proviennent de différents ministères et organismes du gouvernement québécois. Ces personnes sont préparées à intervenir en cas de crise. C'est le CERT/AQ, mentionné précédemment, qui gère ce réseau d'alerte.

Une autre action préventive au Québec consiste à sensibiliser les utilisateurs internes et externes de l'organisation à la sécurité informatique.. Dans certains pays où des sondages et analyses ont été effectués (Allemagne, Royaume-Uni, Lithuanie), il apparaît qu'un des défis actuels consiste à améliorer les connaissances des utilisateurs en matière de sécurité lorsqu'ils utilisent Internet, autant pour le travail que pour des fins personnelles (Wernberg-Tougaard & Bedsted, 2007). Pour la première fois au printemps 2007, le gouvernement du Québec, en collaboration avec l'Institut de sécurité de l'information du Québec (ISIQ)[15] et des organisations des secteurs public, parapublic et privé, a organisé une *Semaine de sensibilisation à la sécurité informatique*. Parmi les activités qui s'y sont déroulées, soulignons la mise en ligne du guide *« Sur Internet, protéger son IDENTITÉ, c'est essentiel ! »*. Ce guide offre aux utilisateurs des moyens concrets d'utilisation d'Internet de façon sécuritaire.

Par ailleurs, afin de sécuriser les transactions avec les citoyens et les entreprises, le gouvernement du Québec a mis en place un service d'authentification nommé *ClicSécur.* Grâce à ce service les utilisateurs qui transigent avec le gouvernement peuvent utiliser un même code d'utilisateur auprès de plusieurs ministères et organismes. Ainsi, ont été jumelées les orientations de sécurité de l'information et de simplification des échanges avec les citoyens et les entreprises.

Outre le gouvernement, d'autres organisations veillent et collaborent à la sécurité informatique de l'État. La Sûreté du Québec a développé un système servant à recueillir les plaintes liées à la cybercriminalité. Les plaintes sont déposées auprès des services de police municipaux, des unités de la Sûreté du Québec ou d'autres agences gouvernementales et civiles. Après avoir vérifié s'il s'agit d'un crime, la plainte est enregistrée. Un enquêteur accumule ensuite les éléments de preuve et s'assure qu'il en possède suffisamment pour engager une enquête. Enfin, les enquêteurs déterminent s'il est possible de retracer le suspect sur Internet. Ce travail est sous la responsabilité du Module de la cybersurveillance et de la vigie (MCV) qui est le pendant québécois du Service canadien de renseignements criminels (SCRC).

Le Service de police de la Ville de Montréal (SPVM) a crée une brigade contre le terrorisme, le Module antiterrorisme et mesures d'urgences (MAMU). Cette brigade élabore des stratégies et des méthodes d'intervention en cas d'événements «tragiques et exceptionnels», qui affecteraient par exemple les infrastructures stratégiques. Cette brigade est responsable de la formation pour ce type d'intervention auprès des policiers du SPVM.

4. DES SYSTÈMES INFORMATIQUES STRATÉGIQUES À SÉCURISER

Les ministères et organismes du gouvernement du Québec disposent de systèmes informatiques qui leur permettent d'offrir plusieurs services en ligne. Selon la nature du service et l'importance de l'information et des transactions, le niveau de sécurité variera. Un système qui offre de l'information publique ne requiert pas le même niveau de sécurité qu'un système qui recueille et possède des renseignements à propos des individus. Le projet de dossier électronique de santé au Québec, appelé dossier de santé du Québec, qui sera implanté d'ici 2010 figure parmi les exemples de systèmes informatiques québécois pour lesquels la sécurité informatique est une préoccupation majeure. Ce dossier doit offrir des garanties suffisantes de confidentialité, d'intégrité et de disponibilité des informations[16]. Outre les enjeux technologiques, ce dossier soulève d'importantes questions en termes de gestion de l'information et des risques. Qui accèdera aux données, de quelle manière et à quel moment? Comment seront conservées les données? Combien de temps le seront-elles? Comment l'usager pourra-t-il être certain que les informations n'ont pas été altérées? Dans quelle mesure et de quelle façon devra-t-il consentir quant à la mise à jour et à la divulgation de son dossier de santé électronique?

Le Registre de l'État civil est un autre exemple de système informatique qui requiert une importante sécurité. Ce registre contient des informations qui pourraient, mises entre de mauvaises mains, permettre de violer des lois et perpétrer des crimes, tel le vol d'identité. C'est pourquoi, en 2006, le Code civil a été revu en ce qui concerne les demandes de documents d'état civil (Gouvernement du Québec, 2006)[17]. Cette révision s'avérait nécessaire puisque les informations détenues au Registre de l'État civil sont à la base l'émission de plusieurs autres documents d'identité permettant de bénéficier de services de l'État. Compte tenu de la nature des informations contenues dans ce Registre, les responsables considèrent qu'il y a pour le moment, trop de risques à mettre un tel registre en ligne et même à traiter en ligne les demandes de documents.

En somme, les systèmes électroniques qui permettent d'offrir des services publics à distance sur tout le territoire québécois ne peuvent pas se permettre de négliger la question de la sécurité informatique. Un crime perpétré sur ces systèmes d'information aurait des impacts financiers et des impacts sur la confiance des citoyens et des entreprises envers l'État.

CONCLUSION

Les nouvelles menaces qui émanent du cyberespace préoccupent tous les États; d'où la mise au point de plusieurs initiatives, tant au plan local qu'à l'échelle internationale. Face à l'augmentation des risques liés à la cybercriminalité, le Québec tente de se prémunir par divers moyens. Des organisations responsables de la sécurité informatique ont été créées et l'adaptation du cadre légal progresse pour tenter de faire face à l'accroissement de l'utilisation d'Internet et aux besoins de sécurité qui y sont associés. De plus, diverses initiatives, telles que la sensibilisation des utilisateurs à la sécurité sur Internet sont lancées. Enfin, l'État québécois favorise la collaboration entre les États et les organisations, privées ou publiques.

Dans l'optique de contribuer davantage à la sécurité informatique et à la coopération dans la lutte contre la cybercriminalité, il serait intéressant que le gouvernement du Québec étudie la question de la ratification par le Canada de la Convention sur la cybercriminalité. Le gouvernement québécois pourrait ensuite effectuer des démarches auprès du gouvernement fédéral pour faire connaître sa position sur cette Convention.

La sécurité informatique soulève biens des questions. Jusqu'où doit-on aller au nom de la sécurité informatique et de la sécurité nationale? La question concernant la protection des renseignements personnels et de la vie privée face à la recherche de sécurité pour l'État et les citoyens pourraient faire l'objet d'un autre rapport. Une autre question importante à explorer concerne la peur qu'instaurent les cyberattaques, voire la crainte du cyberterrorisme. Jusqu'où l'État doit-il pousser la cybersurveillance sans que cela nuise aux droits et libertés individuels et collectifs? L'importance de la protection des infrastructures du secteur énergétique est également évidente. La protection des infrastructures de ce secteur au Québec se veut une piste de réflexion pour un prochain rapport.

Comme l'exprime Ghernaouti-Hélie (2002 : 26), «la sécurité n'est jamais acquise définitivement car la constante évolution des systèmes et des risques rend instable toute mesure de sécurité». Les problèmes de sécurité sont dynamiques et évolutifs, d'autant plus qu'ils se vivent non seulement sur le plan local ou national, mais aussi à l'échelle internationale. Cela ne va pas sans complexifier la tâche des États et des organisations soucieux de réduire les risques et de prévenir l'apparition des menaces. En ce sens, il apparait important d'impliquer tous les acteurs, tant au plan local qu'à l'échelle internationale. La coopération et la concertation entre ces derniers semble être une clé efficace de lutte à la cybercriminalité qui, elle, ne connait pas de frontières.

NOTES

[1]Vocabulaire tiré de la typologie utilisée par la Sûreté du Québec.

[2]*Ibid*.

[3]Le déni de service est une «attaque par saturation d'une entité afin qu'elle s'effondre et ne puisse plus réaliser les services attendus d'elle» Ghernaouti-Hélie, Solange. 2006. *Sécurité informatique et réseaux*.

[4]Selon Ghernaouti-Hélie (2006), la définition du cyberterrorisme n'est pas claire, malgré l'existence d'une certaine uniformité.

[5]Un rapport de l'Inspecteur général de la Défense au États-Unis a révélé des faiblesses dans la sécurité d'un système de paye gouvernemental civil et militaire du *Defense and Veterans Affairs Department*. Ces faiblesses de protection de l'information ne permettent pas au ministère de clamer une sécurité absolue des données qu'il détient. Rosenberg, Alyssa. 2007. «Report cites some gaps en Defense payroll security», *Government Executive.com*, October 9, http://govexec.com/story_page_pf.cfm?articleid=38240

[6]Des données figurant sur les comptes de crédit ont été volées par des fraudeurs. Elles ont été recueillies au moment où les clients retournent des marchandises sans reçu dans les magasins de la société *TJX Companies Inc.* (Commissariat à la protection de la vie privée du Canada. 2007).

[7]Cette recommandation porte le numéro 55/63, 2000.

[8]L'entreprise PandaLabs, Laboratoire antivirus de Panda Software en est un exemple.

[9]CERT™ : *Computer Emergency Response Team*. Inspiré du premier CERT/CC, de l'Université Carnegie Mellon à Pittsburg, créé en 1988.

[10]Quelques lois et politiques canadiennes concernant la sécurité informatique : Loi et politique sur l'accès à l'information, *Loi sur la preuve au Canada, Loi sur la protection civile, Loi sur la protection de l'information, Loi et politique sur la protection des renseignements personnels, Loi sur la protection des renseignements personnels et les documents électroniques (Partie 2), Loi sur le casier judiciaire. Des politiques et d'autres documents administratifs sont également à considérer. Par exemple : Politique d'évaluation, Politique de communication du gouvernement du Canada, Politique sur la sécurité, Politique sur l'autorisation et l'authentification électroniques, Politique sur la gestion des technologies de l'information, Politique sur la vérification interne, Politique sur les services communs.*

[11]Centre national des crimes économiques du Canada (CNCEC), Signalement en direct des délits économiques, https://www.recol.ca/intro.aspx?lang=fr

[12]«Le Québec a signé plus de 200 accords et ententes avec les gouvernements, les villes ou les organismes publics américains. Ces accords portent sur la sécurité, le transport, la culture, le développement économique, le tourisme, l'environnement et l'éducation.» (Ranger, Louis (prés.). 2004 : 238).

[13]Parmi les lois et les politiques à respecter au Québec afin d'assurer la sécurité informatique il faut retenir : Sécurité de l'information gouvernementale, Utilisation éthique du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique , Traitement et destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégé, Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, Lois sur la protection des renseignements personnels dans le secteur privé, Loi concernant le cadre juridique des technologies de l'information.

[14]«La politique de sécurité [définie par une organisation] est l'ensemble des orientations suivies par une organisation en terme de sécurité […] et elle concerne tous les utilisateurs du système». Une politique de sécurité se définit selon 4 étapes : identification des besoins de sécurité; élaboration des règles et procédures; surveillance et détection des vulnérabilités et définition des actions à entreprendre. (Pillou, 2005 :179).

[15]«L'ISIQ est une plateforme publique-privée d'échange d'information et de connaissances en matière de sécurité de l'information». Pour plus d'Information consulter le site de l'ISIQ https://www.isiq.ca/fr/.

[16]«Le dossier de santé regroupera, dans un environnement entièrement sécurisé, les principaux renseignements de santé concernant le citoyen qui y aura consenti. Destiné uniquement aux personnes autorisées, le dossier de santé facilitera le travail des intervenants en fournissant des informations fiables, pertinentes et toujours accessibles tout au long du cheminement du citoyen partout dans le système de santé du Québec» (Santé et services sociaux Québec, *Dossier de santé : pour mieux prendre soin de vous*, (?) : 1

[17]Depuis mars 2006, le Directeur de l'État civil a notamment le droit de vérifier l'identité et l'intérêt d'un demandeur.

Acronymes

APEC	Asia Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
CERT	Computer Emergency Response Team
CERT/AQ	Computer Emergency Response Team de l'administration québécoise
CCRIC	Centre canadien de réponse aux incidents cybernétiques
DES	Dossier électronique de santé
GRC	Gendarmerie Royale du Canada
MAMU	Module antiterrorisme et mesures d'urgences
MCV	Module de la cybersurveillance et de la vigie
MRQ	Revenu Québec
NSA	National Security Agency (États-Unis)
OEA/OAS	Organisation des États d'Amérique
OCDE	Organisation de coopération et de développement économiques
ONU	Organisation des Nations unies
OTAN/NATO	Organisation du Traité de l'Atlantique Nord
RAMQ	Régie de l'assurance maladie du Québec
TIC	Technologies de l'information et des communications
NTIC	Nouvelles technologies de l'information et des communications
SARC	Système automatisé de renseignements sur la criminalité
SCRC	Service canadien de renseignements criminels
SPVM	Service de police de la Ville de Montréal

Bibliographie

Affaires étrangères et Commerce international Canada. 2007. *La cybercriminalité*, http://www.international.gc.ca/foreign_policy/internationalcrime/cybercrime-fr.asp

Agence France-Presse. 2007. «Le gouvernement néo-zélandais cible de cyber-attaques», *Cyberpresse.ca,* mardi 11 septembre, http://www.cyberpresse.ca/article/20070911/CPMONDE/70911050/1014/CPMONDE

Aitoro Jill R. 2007. «Reports of federal security breaches double in four months», *Government Executive.com*, October 23, http://www.govexec.com/story_page.cfm?articleid=38348&dcn=todaysnews

April, Jocelyn. 2006. *Module de la cybersurveillance et de la vigie*, Colloque québécois de la sécurité de l'information, Direction des renseignements criminels, Sûreté du Québec, http://www.asiq.org/CQSI2006/doc/presentations/CQSI20060918JAprlCybersurveillance.pdf

Assemblée nationale. -. «*1.4 Délégation de l'Assemblée nationale pour les relations avec les États-Unis (DANRÉU)» Activités multilatérales du Québec*, http://www.assnat.qc.ca/fra/associations/act-multi.htm#apc

Baillargeon, Stéphane. 2007. «Montréal protège ses réservoirs d'eau contre les terroristes», *Le Devoir,* Vendredi 5 octobre, http://www.ledevoir.com/2007/10/05/159480.html

Chandler, Jennifer A., 2004. «Security in Cyberspace: Combating Distributed Denial of Service Attacks», *University of Ottawa Law & Technology Journal*, 1, 23, 2003–2004 : 233-261.

CEFRIO. 2007. «Sécurité de l'information sur Internet : organismes associés, lois, politiques et programmes d'intervention», *Bulletin e-Veille*, Mai, http://www.msg.gouv.qc.ca/PDF/eveille_rechdoc_mai07.pdf

Centre de Services Partagés du Québec. 2007. *Rapport annuel de gestion 2005-2006*, http://www.cspq.gouv.qc.ca/centre/rapport.asp)

Commissariat à la protection de la vie privée du Canada. 2007. «La brèche dans la protection des données de TJX est attribuable à des mécanismes de sécurité inadéquats, selon les commissaires», *Centre de nouvelles du Canada,* 25 septembre, http://news.gc.ca/web/view/fr/index.jsp?articleid=351019

Commonwealth. 2002. *Model Law On Computer And Computer Related Crime,* Lmm(02)17, http://www.Thecommonwealth.Org/Shared_Asp_Files/Uploadedfiles/%7bda109cd2-5204-4fab-Aa77-86970a639b05%7d_Computer%20crime.Pdf

Conseil de L'Europe. 2001. *Convention sur la cybercriminalité*, http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm

Conseil de L'Europe. 2007. *Convention sur la cybercriminalité STCE no. 185*, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=FRE

Cormier, André. 2005. «L'équipe du CERT/AQ à votre service!», *L'Hyper Média*, Centre de Services Partagés du Québec, septembre, http://www.hypermedia.gouv.qc.ca/scripto.asp?function=validation3&resultat=102654

Cormier, André. 2006. *Présentation du CERT/AQ et du réseau d'alerte*, Centre de Services Partagés du Québec 10 avril, http://www.enpq.qc.ca/pdf/cyber06_certaq.pdf

CRIM. 2004. ISIQ : *Institut de sécurité de l'information (numérique) du Québec*, Présentation, Extrait du plan d'affaires révisé février, http://www.crim.ca/files/documents/services/securite/04.02.25-isiq-sommaire.pdf

EurActiv. 2007. *Dossier Sécurité sur Internet*, 20 septembre. http://www.euractiv.com/fr/societe-information/securite-internet/article-166366

Filiol, Éric et Phillipe Richard. 2006. *Cybercriminalité: Enquête sur les mafias qui envahissent le web*.

G8. 1997. *Communique, Meeting of Justice and Interior Ministers of The Eight*, Washington, December 9-10, Communique Annex: Principles And Action Plan To Combat High-Tech Crime, Statement of Principles http://www.qlinks.net/comdocs/washcomm.htm

Gagnon, Benoit. 2002. «Le cyberterrorisme à nos portes?», *La Presse*, Dimanche 12 mai : A15. http://www.dandurand.uqam.ca/download/journaux/gagnonb/20020512.html

Ghernaouti-Hélie, Solange. 2000. «Stratégie et protection des systèmes d'information», *FI spécial été,* 5 septembre, HEC-Lausanne http://ditwww.epfl.ch/SIC/SA/publications/FI00/fi-sp-00/sp-00-page20.html

Ghernaouti-Hélie, Solange. 2002. *Internet et sécurité*, coll. Que sais-je?

Ghernaouti-Hélie, Solange. 2006. *Sécurité informatique et réseaux*

Gouvernement du Québec. 2007. *Sur Internet, protéger son IDENTITÉ, c'est essentiel !*, http://www.vol-identite.info.gouv.qc.ca/fr/index.asp

Gouvernement du Québec. 2006. *Rapport d'application de la Loi modifiant le Code civil en matière de demande de documents d'état civil* (L.Q. 2001, C. 70)

Hakkaja, Mehis. 2007. «From our own Experts, Mitigation of Massive Cyber Attacks», *ENISA Quarterly*, Vol3, No. 3, July-September: 10, http://www.enisa.europa.eu/doc/pdf/publications/enisa_quarterly_09_07.pdf

ISIQ. 2006. «Simulation de panne informatique généralisée aux États-Unis» *Bulletin*,no 3, Février, http://www.isiq.ca/fr/bulletin/2006/bulletinISIQ_0206.htm

Richard Kissel, (editor). 2006. *Glossary of Key Information Security Terms, National Institute of Standard and Technology - NIST IR 7298*, April 25, http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf

Ministère des Relations internationales (MRI). 2006a. *La politique internationale du Québec; La force de l'action concertée*, Gouvernement du Québec, http://www.mri.gouv.qc.ca

Ministère des relations internationales (MRI). 2006b. *Québec : un partenaire nord-américain en Sécurité*, Gouvernement du Québec, http://www.mri.gouv.qc.ca/fr/pdf/usa_securite.pdf

Ministère des Services gouvernementaux (MSG). 2007a. *Sécurité de l'information*, septembre, http://www.msg.gouv.qc.ca/securite_information/echange.html)

Ministère des Services gouvernementaux (MSG). 2007b. *Directives*, septembre http://www.msg.gouv.qc.ca/fr/securite/directive.asp

Office québécois de la langue française (OQLF). 2007. *Le grand dictionnaire terminologique*, http://www.granddictionnaire.com/btml/fra/r_motclef/index1024_1.asp

Olanié, Marc. 2007. «La France épiée par la Chine», *Réseaux-Télécom.net*, 13 septembre, http://securite.reseaux-telecoms.net/actualites/lire-la-france-epiee-par-la-chine-17083.html

OTAN / NATO. 2002. « Contrer la cyberguerre » *Revue de l'OTAN*, Edition Web, vol. 49, No 4, Hiver 2001/2002: 16-18, http://www.nato.int/docu/revue/2001/0104-04.htm

Panko, Raymond. 2004. *Sécurité des systèmes d'information et des réseaux*

Pillou, Jean-François. 2005. *Tout sur la sécurité informatique*

Ranger, Louis (prés.). 2004. *Création de liens transfrontaliers : un recueil d'information sur la collaboration intergouvernementale Canada-États-Unis,* Table ronde de recherche-action de l'EFPC sur la gestion des relations canado-américaines (Canada), École de la fonction publique du Canada, http://www.coach.gc.ca/Research/publications/pdfs/p128_f.pdf

Ressources naturelles Canada. 2006. Vérification de la sécurité de la technologie de l'information (TI), Rapport (A05010), Direction de la vérification et de l'évaluation, septembre, http://www.nrcan.gc.ca/dmo/aeb/aeb-rpts-2006-A05010-f.htm

Schneier, Bruce. 2000. *Secrets et mensonges, Sécurité numérique dans un monde en réseau*

Scholberg, Stein, (Editor). 2006. *Site CyberCrime Law*, http://www.cybercrimelaw.net/index.html

Secrétariat du Conseil du Trésor (SCT). 2004. *Authentification des citoyens et des entreprises dans le cadre du gouvernement électronique, Orientations et stratégie,* Gouvernement du Québec, Août
http://www.msg.gouv.qc.ca/PDF/strategie_authentification.pdf

Secrétariat du Conseil du Trésor (SCT). 2006. *Politique sur la gestion de l'information,* Gouvernement du Canada, 26 juin,
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/tb_gih/pim-pgi01_f.asp#pim-pgi3

Sécurité publique Canada. 2004. *Exposé de principes*, novembre,
http://www.publicsafety.gc.ca/prg/em/nciap/position_paper-fr.asp

Sécurité publique Canada. 2007. *Centre canadien de réponse aux incidents cybernétiques (CCRIC)*, Gouvernement du Canada,
http://www.sp-ps.gc.ca/prg/em/ccirc/index-fra.aspx

Service canadiens de renseignements criminels (SCRC-CISC). 2007. *Le Système automatisé de renseignements sur la criminalité (SARC*),
http://www.cisc.gc.ca/aciis/aciis_f.htm

Service de Police de la Ville de Montréal. 2007. «Module antiterrorisme et mesures d'urgence», *L'heure juste*, Vol 14, No. 5, 12 juillet : 6,
http://www.spcum.qc.ca/upload/documentations/HJ_2007_07_12.pdf

Simard, André. 2006. *Le dossier de santé du Québec*, Présentation, 28 septembre,
http://www.aqesss.qc.ca/docs/public_html/evenemen/discours/Info_Sante_2006/5Atelier2.pdf

Sûreté du Québec. 2005. «Module de la cybersurveillance et de la Vigie (MCV)», *Cybersurveillance*,
http://www.suretequebec.gouv.qc.ca/lutte/cybersurveillance/cybersurveillance.html

Sûreté du Québec. 2003. *Cheminement des plaintes adressées au MCV*, Direction conseil et développement en enquêtes criminelles, Service développement en enquêtes,
http://www.suretequebec.gouv.qc.ca/publications/pdf/cybersurveillance/cheminement_plainte.pdf

Terrorisme.net. 2002. «Cyberterrorisme, cybercriminalité et cyberguerre : un état de la question en anglais», Archives, 1 décembre, commentaire de Dunnigan, James, F. 2002. *The Next War Zone : Confronting the Global Threat of Cyberterrorism*,
http://www.terrorisme.net/lecture/2002/008_cyberterror_dunnigan.htm

Wernberg-Tougaard, Christian and Bjørn Bedsted. 2007. «IT Security Beyond Borders»,
ENISA Quarterly Vol. 3, No. 3, July-September: 14-16,
http://www.enisa.europa.eu/doc/pdf/publications/enisa_quarterly_09_07.pdf

LEPPM

Le Laboratoire d'étude sur les politiques publiques et la mondialisation a été créé en 2004 par une entente de partenariat entre le Ministère des Relations internationales et l'ENAP. Le Laboratoire est un lien de veille et d'analyse consacré à l'étude des effets de la mondialisation sur le rôle de l'État, et sur les politiques publiques au Québec, et ce sur les enjeux d'ordre culturel, économique, environnemental, de santé, d'éducation et de sécurité. Il est apparu essentiel de répondre à cette préoccupation des impacts de la mondialisation sur la vie des institutions, des entreprises et de la société québécoise.

Directeur par intérim : Paul-André Comeau

Pour plus d'information ou si vous avez des renseignements à nous transmettre, vous pouvez contacter :

la technicienne du Laboratoire
Téléphone : (418) 641-3000 poste 6864
leppm@enap.ca

Les publications du Laboratoire peuvent être consultées sur le site Internet :

www.leppm.enap.ca

Relations internationales
Québec

École nationale d'administration publique