Public Safety and Emergency Preparedness Canada
Sécurité publique et Protection civile Canada

La responsabilité dans le domaine de l'infrastructure d'information essentielle au Canada

Canada

Remerciements

Cette publication a été établie pour :

Sécurité publique et
Protection civile Canada

340, avenue Laurier Ouest, 12e étage
Ottawa (Ontario) K1A 0P8
Internet : www.psepc-sppcc.gc.ca

Auteurs :

Donald B. Johnston – Chef de projet
Robert Fabian
Keith L. Geurts
Donald S. Hicks
Andrew Huzar
Norman D. Inkster
Alan Jaffee
Paul McLennan
Douglas J. Nash
E. Michael Power
Mark Stirling

Gowling Lafleur Henderson LLP
Avocats-conseils
Agents de brevets et marques de commerce
Pièce 5800, Scotia Plaza
40, King Street West
Toronto (Ontario) Canada M5H 3Z7
Téléphone : 416-369-7200

Ce document se fonde sur des travaux corroborés par la Division de la recherche et du développement (DRD) au Bureau de la protection des infrastructures essentielles et de la protection civile (BPIEPC) dans le cadre du contrat no 2003D022. Le 12 décembre 2003, le Bureau de la protection des infrastructures essentielles et de la protection civile a été intégré à un nouveau ministère, Sécurité publique et Protection civile Canada (SPPCC). Les opinions, les résultats et les conclusions ou les recommandations exprimées dans ce document sont celles de l'auteur ou des auteurs et ne reflètent pas nécessairement les points de vue de Sécurité publique et Protection civile Canada.

Catalogue no : PS48-7/2004F-PDF
ISBN : 0-662-77867-7

Note du traducteur : Traduction libre des citations, à l'exception de celles qui sont extraites de lois canadiennes ou de certains textes traduits. Selon les indications reçues, les références à d'autres documents, les adresses de sites Web et la bibliographie ne sont pas traduites.

Sommaire

OBJECTIFS

Tout au long de notre recherche approfondie, il y a eu un large consensus selon lequel le Canada dépend de plus en plus de l'infrastructure d'information à la fois pour notre sécurité et pour le fonctionnement de notre société. À mesure que notre dépendance envers cette infrastructure essentielle augmente, les questions de responsabilité deviennent plus importantes.

Dans ce rapport, nous donnons une vue d'ensemble des idées actuelles sur l'infrastructure d'information essentielle au Canada et nous examinons en outre la vaste gamme de questions et de préoccupations qui ont trait à la responsabilité. Plus précisément, nous examinons les points suivants :

1. L'état actuel et l'évolution future de l'infrastructure d'information;
2. Le concept de responsabilité en ce qui a trait à l'infrastructure d'information essentielle;
3. Les mécanismes de responsabilité actuellement en place qui touchent l'infrastructure d'information essentielle;
4. Les leçons en matière de responsabilité tirées d'autres environnements qui peuvent être pertinentes pour l'infrastructure d'information essentielle;
5. L'état actuel de la responsabilité dans le domaine de l'infrastructure d'information essentielle au Canada tel qu'il est perçu par les principaux intéressés;
6. Les principales questions et préoccupations au sujet de la responsabilité et
7. Les propositions qui visent à améliorer la fiabilité, la sécurité et la fonctionnalité de l'infrastructure d'information essentielle.

LA RECHERCHE

Nous avons mené des entrevues par téléphone avec les principaux intéressés au Canada et aux États-Unis concernant les points énumérés ci-dessus. Nous avons également entrepris beaucoup de recherches secondaires. Les documents que nous avons examinés sont cités dans la section Bibliographie du présent rapport.

DÉVELOPPEMENT DE L'INFRASTRUCTURE D'INFORMATION

Le rapport comprend une section sur l'historique de l'infrastructure d'information actuelle au Canada. Cette section traite également des tendances en matière de développement de chacun des composants clés de l'infrastructure d'information, soit le matériel, les logiciels, les réseaux et les services. De grandes projections technologiques, jusqu'en 2020, donnent le contexte de l'avenir.

L'Internet est une source importante d'idées et de technologies à utiliser dans notre infrastructure d'information. L'Internet est également un composant de l'infrastructure d'information essentielle et une ressource clé qui doit être utilisée dans l'infrastructure d'information essentielle du Canada. Nous incluons un bref historique de l'Internet aux États-Unis et au Canada, en accordant une attention particulière à la période qui suit 1994, soit au moment où l'utilisation commerciale de l'Internet a été permise.

La loi de Moore sert à expliquer de nombreux développements passés et futurs du matériel. Le logiciel est expliqué selon les générations de programmation qui ont mené aux possibilités de

programmation visuelles d'aujourd'hui où le diagramme d'un programme *est* le programme. Les réseaux sont examinés en fonction des principaux changements qui seront probablement observés. L'histoire des services aujourd'hui est essentiellement celle de l'externalisation, à l'intérieur, à proximité et au loin.

La projection technologique jusqu'en 2020 s'appuie fortement sur une étude RAND faite par les forces militaires des États-Unis. Selon cette étude, d'ici 2020, il y aura une distinction de plus en plus floue entre les objets physiques et leur image cybernétique. Les technologies sans fil seront omniprésentes et offriront des connexions à grande capacité. Le matériel trouvera les moyens de continuer à suivre la loi de Moore. Le réseau sera notre connexion universelle. Nous donnons une récapitulation des résultats du rapport RAND.

OBJECTIFS DE LA RESPONSABILITÉ DANS LE DOMAINE DE L'INFRASTRUCTURE D'INFORMATION ESSENTIELLE

Voici quelques-unes des questions que l'équipe chargée de la recherche a posées afin de mieux comprendre toute l'infrastructure d'information essentielle ainsi que le rôle actuel, éventuel ou possible de la responsabilité dans ce domaine :

1. Comment le niveau ou l'attribution des responsabilités entre les participants de l'infrastructure d'information essentielle touchent-ils le développement et le fonctionnement de l'infrastructure d'information essentielle?

2. De quelles façons la responsabilité a-t-elle contribué à un état souhaitable, ou indésirable, de l'infrastructure d'information essentielle?

3. Quels attributs décrivent le mieux l'infrastructure d'information essentielle actuelle et future et quelles sont les mesures correspondantes?

4. Quelle est la recherche actuelle au sujet de chacun de ces attributs et que faudrait-il savoir d'autre?

5. Comment et de quelle façon l'état futur voulu de l'infrastructure d'information essentielle est-il lié à chacun des attributs?

6. Quelles sont les relations entre les divers attributs pertinents de l'infrastructure d'information essentielle et quelles sont les solutions de compromis entre eux?

7. Quelles sont les relations, y compris les solutions de compromis, entre les divers attributs de l'infrastructure d'information essentielle et les politiques qui les gouvernent?

Notre recherche a fortement indiqué qu'il y a deux mécanismes qui peuvent aider à améliorer la fiabilité et la fonctionnalité de l'infrastructure d'information essentielle, soit la diversité et la responsabilité. Dans un monde parfait, nous pourrions avoir une infrastructure d'information essentielle qui comprend un certain nombre de composants divers, mais équivalents fonctionnellement, à chacun des niveaux. Nous pourrions avoir des responsabilités claires et pertinentes pour tous les aspects. Cela nous donnerait deux mécanismes distincts de sûreté

intégrée. Toutefois, dans le monde réel, il peut y avoir des difficultés à atteindre une certaine diversité et des niveaux élevés de responsabilité.

RESPONSABILITÉ DANS D'AUTRES ENVIRONNEMENTS

Le défi d'avoir le « bon » degré de responsabilité pour les infrastructures essentielles est universel. Ce défi s'applique à la fois à d'autres infrastructures essentielles et à d'autres juridictions. De nombreuses leçons ont été apprises à partir d'initiatives précises et de l'évolution générale de la responsabilité. Nous estimons qu'un certain nombre de ces leçons peuvent être pertinentes pour la responsabilité dans le domaine de l'infrastructure d'information essentielle et nous allons traiter de cette pertinence.

Services de santé et services juridiques

Les professions sont en mesure de définir des normes et de les faire appliquer. La menace de réglementation assure l'intégrité. Des normes professionnelles peuvent être nécessaires si nous devons atteindre un niveau important de responsabilité dans l'infrastructure d'information essentielle.

Services financiers

La réglementation dans le secteur public peut être requise dans certaines circonstances. Dans des environnements évolutifs connectés mondialement, des processus formels peuvent être requis, avec des examens périodiques et des mises à jour. Il faudra sans doute établir des mesures et des processus convenus pour tenir les entités responsables. Finalement, lorsqu'une entité ne contrôle pas toutes les entrées, le type le plus efficace de responsabilité est souvent celui des processus.

Services d'électricité

La seule approche pratique est peut-être celle de la responsabilité quant aux résultats, à l'interface entre les systèmes privés et le système partagé plus vaste. L'interface offre un point de mesure. L'infrastructure d'information essentielle se compose de nombreux systèmes privés qui ont une interface avec un vaste système partagé. Les opérateurs des systèmes privés pourraient être tenus responsables s'ils « exportent leurs ennuis » vers le système partagé.

An 2000

Notre succès collectif dans le cas de l'An 2000 peut être une source de fierté, mais il n'y aucune raison nécessaire de supposer que la même approche servirait à protéger l'infrastructure d'information essentielle au Canada. Même si l'approche An 2000 ne s'applique pas particulièrement à l'infrastructure d'information essentielle, elle donne un exemple de la façon dont une menace perçue comme suffisamment grave peut galvaniser à la fois le secteur public et le secteur privé et les pousser à prendre des mesures efficaces.

Commission Treadway/Sarbanes-Oxley

Comprendre un problème éventuel sérieux n'est pas suffisant. Identifier une solution n'est pas suffisant. La solution doit être mise en œuvre. Cela prend des ressources et de la volonté, toutes choses qui ne sont pas faciles à générer en l'absence d'un désastre. Lorsque les désastres se produisent sous forme de scandales financiers importants (par exemple, Enron et WorldCom), les ressources peuvent se matérialiser. Sarbanes-Oxley en a été le résultat.

Directive de l'Union européenne/Loi sur la protection des renseignements personnels et les documents électroniques
Des initiatives dans une juridiction peuvent générer des initiatives positives correspondantes dans d'autres juridictions. L'infrastructure d'information essentielle du Canada fait partie de l'infrastructure d'information mondiale. Les initiatives que le Canada décide d'entreprendre peuvent bénéficier au Canada et générer ailleurs des bénéfices positifs correspondants.

HIPAA (Health Insurance Portability and Accountability Act)
L'économie n'est peut-être pas le seul ou principal facteur de changement important. La loi américaine HIPAA fournit un contre-exemple convaincant. Des initiatives qui ne sont pas populaires auprès de quelques-uns peuvent réussir grâce à un appui suffisant de la population. Des changements apportés au cadre de responsabilité de l'infrastructure d'information essentielle peuvent ajouter plus de coûts que de profits, mais l'expérience de la loi HIPAA montre que cela ne constitue qu'un seul facteur dans la prise de décision et non le facteur décisif.

MÉCANISMES DE RESPONSABILITÉ DANS LE DOMAINE DE L'INFRASTURES D'INFORMATION ESSENTIELLE

La responsabilité est un concept à plusieurs facettes. Afin d'étudier la responsabilité dans le domaine de l'infrastructure d'information essentielle, le rapport examine de façon très détaillée deux aspects importants de la responsabilité. Il y a l'examen du mécanisme courant qui sert à réaliser le cadre de responsabilité en vertu de la loi canadienne et dans les marchés canadiens. Il y a aussi l'examen des mécanismes de responsabilité qui sont fortement utilisés dans les marchés établis pour les produits et services qui constituent l'infrastructure d'information essentielle.

Les mécanismes courants de responsabilité remontent aux idées plus fondamentales de l'indemnisation et de l'indemnité. Le rapport inclut une définition simplifiée de l'indemnité, soit « un accord selon lequel une partie consent à protéger une autre partie contre toute perte ou dommage prévu ». La question devient alors celle de l'examen des méthodes courantes selon lesquelles l'indemnisation est réalisée en vertu de la loi canadienne et dans les marchés canadiens. Le rapport traite spécifiquement de l'indemnisation dans le domaine des logiciels, des systèmes, des services et du matériel.

En gros, trois mécanismes sont examinés, soit le droit de la responsabilité délictuelle, le droit pénal et l'assurance. Le droit de la responsabilité délictuelle est généralement utilisé lorsque la partie lésée peut obtenir une indemnité de la partie qui a causé le préjudice. La cause du préjudice peut être due à la négligence et c'est alors une source de débats et de discussions sans fin car la négligence comporte des éléments fortement subjectifs. Il y a encore un grand nombre de questions sans réponse au sujet de la façon dont le droit de la responsabilité délictuelle pourrait s'appliquer à des pertes en relation avec notre infrastructure d'information essentielle.

Le droit pénal adopte une approche différente. Il traite des actes qui sont censés être des crimes en vertu du *Code criminel* du Canada. En suivant ce type de raisonnement, le rapport cite la définition de crime informatique de la GRC, soit « tout acte illégal au cours duquel le système informatique devient l'objet d'un crime ou en est l'instrument ou sert de dépôt de preuves liées à un crime ». Le rapport examine la façon dont cela touche les trois acteurs les plus importants, soit le législateur, l'exécuteur et le criminel.

La question de l'assurance a donné lieu à des avis tranchés au cours de nos entrevues avec les participants. Certains participants estimaient que l'assurance pouvait jouer un rôle pivot dans la protection de l'infrastructure d'information essentielle et c'était souvent des cadres dans le domaine de l'assurance qui étaient très fortement et directement intéressés à l'affaire. Le rapport considère de manière assez approfondie comment, pourquoi, où et quand l'assurance peut être employée (ou non) pour améliorer la sécurité, la disponibilité et la fiabilité de notre infrastructure d'information essentielle. Malgré les promesses perçues par certains participants, il y a encore un certain nombre de questions importantes qui sont sans réponse.

Le rapport examine ensuite les responsabilités que l'on trouve couramment en relation avec les logiciels, les systèmes, les services et le matériel. Le point de départ consiste à étudier les responsabilités dans le cas des produits logiciels, des logiciels personnalisés et des systèmes (logiciels). Ces points de référence ont été choisis pour illustrer la gamme de responsabilités que l'on trouve sur le marché canadien actuel. La plus grande partie de ce qui peut être observé, ce sont les moyens par lesquels les fournisseurs ont pu fortement limiter les responsabilités qu'ils doivent assumer.

Des progrès ont été réalisés dans l'attribution appropriée des responsabilités en relation avec les services des technologies de l'information (TI). La norme BITI (Bibliothèque de l'infrastructure des technologies de l'information (aussi appelée ITIL)) fournit un cadre de travail largement accepté pour la prestation et la gestion des services TI. En outre, la norme BITI a identifié les moyens par lesquels les responsabilités peuvent être attribuées. Les outils sont disponibles pour l'attribution des responsabilités, mais ils ne sont pas souvent mis en pratique. Dans le cas du matériel, les pratiques observées limitent fortement les responsabilités.

ÉTAT ACTUEL DE LA RESPONSABILITÉ DANS LE DOMAINE DE L'INFRASTRUCTURE D'INFORMATION ESSENTIELLE

Tous les participants que nous avons interrogés nous ont dit qu'ils croyaient qu'il y aurait au moins une panne majeure de l'infrastructure d'information essentielle dans les cinq prochaines années. Certains participants informés ont été même jusqu'à soutenir qu'une panne de l'infrastructure d'information était l'une des principales causes de la grande panne d'électricité de 2003.

La question de la monoculture de Microsoft a été soulevée dans un certain nombre d'entrevues avec les participants – les monocultures sont fragiles et nous avons une monoculture de bureau Microsoft. Microsoft peut avoir « causé » le monopole de bureau, mais ce qui devrait être fait à ce sujet, le cas échéant, n'est pas très clair. Plusieurs participants ont signalé les avantages qu'il y aurait à encourager la diversité.

Au cours de nos entrevues, les participants ont fortement appuyé l'idée qu'il y a de puissantes interdépendances entre des juridictions adjacentes, comme entre le Canada et les États-Unis. Pour que des mesures soient efficaces, il faudrait sans doute les coordonner à l'échelle internationale. Le Canada n'est pas libre d'agir tout seul, mais d'autres peuvent être prêts à voir le Canada jouer un rôle de premier plan.

L’absence de professionnels, comme dans les domaines de la médecine et de la comptabilité, a été perçue par plusieurs participants comme une limitation sérieuse de ce qui peut être fait pour améliorer notre infrastructure d’information essentielle. Toutefois, avant d’accepter de nouvelles catégories de professionnels, tout le monde s’entendait pour dire que nous devons établir et accepter des normes pertinentes sur l’exercice de la profession. Il serait bon d’envisager et d’encourager l’établissement de telles normes.

Au cours de nos entrevues, il y a eu un consensus surprenant au sujet du rôle que le gouvernement devrait jouer. Les participants ont convenu que le gouvernement ne devrait pas jouer le rôle principal. Il pourrait assurer le financement et encourager des développements prometteurs, mais tout rôle central du gouvernement a été envisagé avec un degré élevé de scepticisme.

Malgré la réticence à voir le gouvernement jouer le rôle principal, les participants ont reconnu que le financement public serait requis. En outre, ils ont estimé qu’il fallait se concentrer davantage sur ce qui devait être fait pour maintenir, améliorer et soutenir l’infrastructure d’information essentielle. Il y avait aussi un sentiment bien clair que cette préoccupation au sujet de notre infrastructure d’information essentielle devrait être largement reconnue dans tout le Canada.

Après un bref examen des difficultés internationales actuelles dans le domaine de l’Internet, il en est ressorti que l’on accepte très peu la responsabilité dans le cas des services partagés ou publics de bout en bout de l’infrastructure d’information au Canada. La pensée bien ancrée contre la réglementation de l’Internet devrait être prise en considération lorsqu’il s’agit d’établir ces responsabilités, si jamais on détermine qu’elles sont souhaitables.

OBSTACLES À LA RESPONSABILITÉ

Il est important de comprendre les barrières pratiques qui peuvent être érigées si jamais on décide d’introduire des responsabilités additionnelles dans le domaine de l’infrastructure d’information essentielle au Canada. En profitant de l’expérience approfondie de l’équipe de recherche sur le plan juridique et consultatif, nous avons établi une liste préliminaire des obstacles pratiques possibles, soit :

- Responsabilité diluée
- Coûts accrus des produits et services
- Coûts accrus d’application des lois et règlements
- Réduction du rythme d’innovation
- Limitations de la sphère d’influence du Canada
- Normes manquantes, à la fois dans les mesures et dans les pratiques
- Résistance humaine naturelle au changement
- Nécessité d’un désastre pour inspirer de l’action
- Difficulté à identifier l’infrastructure d’information essentielle
- Compréhension incomplète de l’infrastructure d’information essentielle

CARACTÉRISTIQUES DU MODÈLE DE RESPONSABILITÉ

Étant donné que l'équipe de recherche estimait qu'il faudrait sans doute envisager des responsabilités accrues dans le cas de l'infrastructure d'information essentielle au Canada, nous étions d'avis qu'un *modèle de responsabilité* pouvait être requis à l'avenir. Nous avons puisé dans notre expérience de consultation et de gestion pour identifier les *dimensions* qui pourraient servir à bâtir un modèle de responsabilité et les *mécanismes* que l'on pourrait utiliser pour établir les niveaux voulus de responsabilités.

Dimensions de la responsabilité

- Genres de responsabilités
- Raisons d'accepter la responsabilité
- Parties qui acceptent la responsabilité
- Procédures d'application
- Conséquences des défaillances

Mécanismes de responsabilité

- Défense de l'intérêt public
- Achats prescrits
- Établissement de normes
- Application des normes
- Licence professionnelle ou autorisation d'exercer la profession
- Réglementation du marché
- Réglementation directe

APPROCHES POSSIBLES POUR AMÉLIORER L'INFRASTRUCTURE D'INFORMATION ESSENTIELLE

Notre recherche a mis en lumière quatre domaines qui pourraient être pris en considération lorsque nous explorons la façon d'améliorer la fiabilité, la sécurité et la fonctionnalité de l'infrastructure d'information essentielle. Les suggestions suivantes représentent la synthèse des opinions des principaux participants. Elles devraient toutes faire l'objet de recherches et de consultations approfondies avant de songer à la mise en œuvre.

Encourager la diversité dans l'infrastructure d'information partagée

La diversité, bien encouragée, peut améliorer la fiabilité de l'infrastructure d'information globale au Canada. Il peut y avoir des avantages importants avec plusieurs instances de composants différents et distincts et cependant fonctionnellement équivalents à chaque niveau de l'infrastructure d'information partagée.

Appliquer la responsabilité dans le cas de l'infrastructure d'information partagée

Une plus grande responsabilité pourrait être imposée à ceux qui bâtissent et qui exploitent des services partagés dans l'infrastructure d'information. Comme ces services sont le résultat du travail de collaboration de nombreux acteurs, la plupart des responsabilités seront probablement imposées pour les processus.

Appliquer la responsabilité dans le cas de l'infrastructure d'information privée
Ceux qui exploitent des services privés connectés à l'infrastructure d'information partagée pourraient avoir une plus grande responsabilité. Comme ces services sont largement sous la responsabilité de ceux qui les exploitent, la plupart des responsabilités pourraient être celles des résultats. Les résultats sont en général mesurés de la meilleure façon possible à l'interface entre le service privé et l'infrastructure d'information partagée.

Encourager l'établissement et l'adoption de normes
En général, les normes sont utiles à la mise en œuvre de la responsabilité. Les normes nous permettent de mesurer, de certifier et d'interconnecter des éléments de l'infrastructure d'information. Les normes internationales peuvent être les plus importantes à cause de la nature mondiale de l'infrastructure d'information, mais les normes canadiennes peuvent également jouer des rôles importants.

LACUNES DU SAVOIR

Si l'infrastructure d'information essentielle doit continuer à évoluer et à se développer sur le plan des fonctionnalités, de la solidité et de la sécurité, nous devrions envisager les mérites qu'il y a à améliorer la gouvernance globale et la responsabilité dans le domaine de l'infrastructure d'information essentielle. Nous serons dans une bien meilleure position pour une telle amélioration si nous comblons les lacunes critiques de notre savoir. Voici quelques exemples sélectionnés :

- Identifier l'infrastructure d'information essentielle
- Identifier toute la gamme des participants et leurs positions
- Comprendre les interactions des composants de l'infrastructure d'information
- Faire des extrapolations quant à l'évolution de l'assurance cybernétique

Table des matières

1.0 Objectifs

Ce rapport nous fait avancer un pas de plus dans la voie de la compréhension de l'infrastructure d'information essentielle. C'est une voie importante. En tant que Canadiens, nous devenons de plus en plus dépendants de l'infrastructure de l'information à la fois pour notre sécurité et pour le fonctionnement de notre société.

Nous avons entrepris cette étude sans aucun préjugé sur ce qui devrait être appris et sans un ordre du jour spécifique à soutenir. Voici quelques-uns des domaines que nous voulions examiner :

1. L'état actuel et l'évolution future de l'infrastructure d'information;
2. Le concept de responsabilité en ce qui a trait à l'infrastructure d'information essentielle;
3. Les mécanismes de responsabilité actuellement en place qui touchent l'infrastructure d'information essentielle;
4. Les leçons de responsabilité pertinentes tirées d'autres environnements;
5. L'état actuel de la responsabilité dans le domaine de l'infrastructure d'information essentielle au Canada, tel qu'il est perçu par les principaux participants;
6. Les principales questions de responsabilité et
7. Les suggestions visant à améliorer la fiabilité, la sécurité et la fonctionnalité de l'infrastructure d'information essentielle.

Nous avons reconnu dès le départ qu'il y avait plusieurs points importants à garder à l'esprit pendant ce projet :

1. Il n'existe aucune définition précise, faisant l'unanimité, des termes infrastructure d'information et infrastructure d'information essentielle, et le but de ce rapport n'est pas d'en fournir une. Dans ce rapport, nous utiliserons la définition généralement acceptée selon laquelle l'infrastructure d'information regroupe un large éventail de technologies, de services et de secteurs de l'industrie, y compris l'informatique, les réseaux, les logiciels, l'Internet, les télécommunications et plusieurs autres. Les différences précises entre ce qui constitue ou non une infrastructure d'information pourront faire l'objet d'autres travaux, mais ce n'est pas ce qui nous préoccupe pour le moment.
2. Le rapport peut donner lieu à des débats sur les changements à apporter à la responsabilité dans le domaine de l'infrastructure d'information essentielle. C'est un sujet controversé. De très grandes quantités d'argent sont en jeu, à la fois à l'intérieur du pays et à l'échelle internationale.
3. Le niveau de préoccupation croît rapidement dans de nombreux secteurs au sujet des effets de pannes importantes de l'infrastructure d'information essentielle. Cette préoccupation pourrait attiser une demande croissante quant aux mesures à prendre.
4. Le rapport peut indiquer les voies possibles pour aller de l'avant, mais il ne pourra pas présenter de solutions définitives. Beaucoup d'enquêtes et de consultations additionnelles doivent être menées avant que des mesures prudentes puissent être recommandées.
5. L'infrastructure d'information en est encore à ses débuts. Les législateurs, les organismes de réglementation, les associations et les utilisateurs n'ont pas encore eu suffisamment de temps pour régler les questions de responsabilité.

6. L’infrastructure d’information essentielle est une cible en rapide évolution. Les « solutions » statiques deviennent désuètes aussitôt qu’elles sont proposées. Il faut un cadre de travail qui puisse adapter continuellement les solutions aux besoins du moment.
7. L’infrastructure d’information essentielle est un énorme sujet. Les limitations en matière de ressources nous ont obligés à restreindre la portée du projet.

2.0 Méthodologie

2.1 Comment ce rapport a été établi

Nous avons commencé par un énoncé clair des objectifs, mais sans aucun préjugé sur ce qui devait être appris et sans aucun ordre du jour spécifique à soutenir. Comme il a été indiqué dans la section précédente, les objectifs ont été raffinés conjointement avec Sécurité publique et Protection civile Canada (SPPCC) à mesure que le rapport progressait.

Pour définir la portée du rapport, nous avons compilé une ébauche de la table des matières. La table des matières a été modifiée et élargie tout au long du projet pour la tenir alignée sur les objectifs. Nous avons essayé de déterminer quelle est l'information qui devrait être idéalement traitée dans chaque section et comment cette information pouvait être obtenue. Cela nous a menés à établir un plan de recherche que nous avons intégré au plan global du projet.

Après avoir bien saisi la portée du projet, nous avons réuni une équipe multidisciplinaire qui avait les connaissances spécialisées nécessaires à l'exécution du projet tel qu'il était prévu. La responsabilité de chaque section du rapport a été attribuée au membre de l'équipe qui avait l'expertise appropriée. Grâce à cette attribution rapide des tâches, chaque membre de l'équipe a pu diriger ses sections comme des mini-projets au sein du travail global. Un gestionnaire de projet a assuré la coordination des travaux des membres de l'équipe.

Nous avons entrepris une grande recherche secondaire. Cela nous a donné une base solide d'information et nous a permis également de découvrir les principales organisations dans le domaine de l'infrastructure d'information. Les résultats de cette recherche sont récapitulés dans la section Bibliographie de ce rapport.

Une initiative de recherche primaire a complété notre recherche secondaire. Nous avons identifié des leaders d'opinion dans divers types d'organisations clés et nous avons mené des entrevues fortement ciblées pour déterminer l'étendue des idées au sujet de la responsabilité dans le domaine de l'infrastructure d'information essentielle. Nous avons exclu les représentants du secteur public de notre cadre d'échantillonnage des entrevues afin de nous concentrer sur le secteur privé et le secteur sans but lucratif. Nous avons trouvé qu'il y avait un degré élevé de réticence au sujet de la participation aux entrevues. Cette réticence était générale et ce n'était pas parce que les gens étaient trop occupés. La responsabilité est clairement un sujet sensible que de nombreuses personnes préféreraient ne pas aborder. Dans l'ensemble, nous avons demandé des entrevues à 108 personnes. Vingt-quatre ont accepté de participer et ont été interrogées.

En parallèle avec notre recherche secondaire et avec les entrevues, nous avons mené une série de sessions internes de réflexion pendant tout le projet. Ces sessions ont donné lieu à des pensées originales et nous ont aidés à garder nos efforts concentrés sur les objectifs.

Nous faisions le suivi du projet au cours de réunions d'étape hebdomadaires dont les résultats étaient documentés et distribués à l'équipe. Ces réunions nous ont permis de déterminer rapidement les nouveaux défis.

Des communications fréquentes avec SPPCC, à la fois formelles et informelles, nous ont permis d'assurer une approche de collaboration pendant tout le projet. À mesure que les premières

ébauches des sections de rapport étaient produites, nous les partagions avec SPPCC pour avoir les commentaires des responsables au Ministère. Cela nous a donné le maximum de souplesse pour faire des ajustements à mesure que le rapport prenait forme. Après la rédaction de la première ébauche, une révision technique détaillée a été effectuée par un tiers qualifié. SPPCC a examiné l'ébauche et formulé des commentaires, qui ont été intégrés, comme convenu, au rapport final.

2.2 Points divers

En consultation avec SPPCC, nous avons choisi de suivre la norme du Manuel canadien de la référence juridique pour toutes les notes en bas de page du rapport. Toutes les pages Web citées en bas de page et la bibliographie étaient actives au 18 mars 2004.

À moins d'indication contraire, toutes les références aux lois et aux organisations sont censées être des références canadiennes.

3.0 Développement de l'infrastructure d'information

3.1 Historique de l'Internet

Toute l'histoire de l'informatique pourrait être intégrée à ce rapport pour indiquer le contexte qui a mené à l'infrastructure d'information actuelle du Canada. Il est intéressant de noter que l'ordinateur UTEC[1] 1952 de l'Université de Toronto a fourni au Canada l'un des premiers ordinateurs en exploitation en Amérique du Nord. Il est également intéressant de savoir que le Commodore canadien 64[2], lancé à l'exposition 1977 Consumer Electronics Show, a précédé de plusieurs mois les appareils Apple II et Radio Shack TRS80. Le Commodore a été le premier « véritable » ordinateur à réussir des ventes importantes dans le commerce de détail.

Ce sont là des faits intéressants au sujet de l'histoire de l'informatique au Canada[3]. Pendant la plus grande partie de cette histoire, il n'y avait rien que l'on pouvait appeler Infrastructure d'information au Canada. Il y avait un nombre croissant de réseaux d'ordinateurs canadiens dans les années 1970 et 1980, mais c'était difficile et coûteux d'établir des connexions entre ces premiers réseaux. L'introduction en 1994 de l'utilisation commerciale[4] de l'Internet au Canada a changé tout cela. De plus en plus de réseaux canadiens ont suivi le protocole Internet IP (Internet Protocol)[5]. L'interconnexion des réseaux est devenue de plus en plus courante, ce qui a donné naissance à l'infrastructure d'information canadienne.

3.1.1 Développements de l'Internet à l'échelle mondiale

Il y a un ensemble important et toujours croissant d'ouvrages sur l'Internet. La recherche[6] de livres sur le sujet « Internet » dans amazon.ca a donné 20 795 résultats. Heureusement, un bon nombre des responsables du développement de l'Internet sont encore vivants et actifs. « A Brief History of the Internet[7] » décrit les débuts de l'Internet, tels qu'ils sont racontés par les personnes qui l'ont établi. Très tôt dans l'utilisation des ordinateurs, des penseurs éminents ont reconnu le potentiel de réseaux d'ordinateurs à grande échelle.

---

[1]Michael R. Williams, « UTEC and Ferut: The University of Toronto's Computation Centre » *IEEE Annals of the History of Computing* 16:2 (été 1994).

[2]Ian Matthews, « The Amazing Commodore PET » *Commodore Business Machines Product Line Up* (22 février 2003), en ligne : Ordinateurs Commodore <http://www.commodore.ca/products/pet/commodore_pet.htm>.

[3]La CBC a une section d'archives intitulée « Computer Invasion: A History of Automation in Canada ». On y trouve l'histoire anecdotique de l'informatique au Canada. On peut la voir en ligne à <http://archives.cbc.ca/IDD-1-75-710/science_technology/computers/>.

[4]Avant 1994, le modèle de financement de l'Internet aux États-Unis interdisait l'utilisation du réseau à des fins commerciales. Avant 1994, l'Internet servait exclusivement à des fins universitaires, gouvernementales (et militaires). Après 1994, l'usage commercial a été permis.

[5]« Le protocole Internet IP est une méthode normalisée de transport de l'information en paquets de données sur l'Internet. Ce protocole est souvent lié au protocole de contrôle de transmission TCP qui assemble les paquets une fois qu'ils ont été livrés à la destination voulue. » Voir en ligne *Campus Information Technologies and Educational Services - Glossary of Acronyms and Technical Terms* <http://www.cites.uiuc.edu/glossary/#i>.

[6]La recherche a été menée le 27 février 2004.

[7]Vinton G. Cerf *et al*., « A Brief History of the Internet » *Internet Histories* (10 décembre 2003), en ligne : Société Internet <http://www.isoc.org/internet/history/brief.shtml>.

> La première description enregistrée des interactions sociales qui pouvaient se faire grâce à l'interconnexion de réseaux était une série de notes de service écrites en août 1962 par J.C.R. Licklider de MIT et qui traitait du concept de « Réseau galactique ». Il envisageait un ensemble mondialement interconnecté d'ordinateurs dans lesquels tout le monde pouvait rapidement accéder à des données et à des programmes à partir de n'importe quel site. Dans le fond, le concept ressemblait énormément à l'Internet d'aujourd'hui[8].

À ce moment-là, le seul grand réseau était celui du système téléphonique. Ce réseau utilisait des circuits de commutation pour établir une connexion continue entre deux parties qui communiquaient entre elles. Si un réseau plus grand utilisait cette approche, il devait fonctionner à l'aide d'un point central de commutation. Ce point central de commutation risquait de devenir rapidement *le* goulot d'étranglement du réseau. Une autre approche a été proposée par Leonard Kleinrock en 1961[9]. Cette approche utilisait les paquets de données.

L'idée semble maintenant évidente. Tous les ordinateurs devaient se connecter à un réseau partagé. L'ordinateur A parlerait à l'ordinateur B en envoyant des paquets d'information adressés à B dans le réseau partagé. Seul l'ordinateur B lirait les paquets qui lui étaient destinés. L'idée était révolutionnaire, particulièrement pour les ingénieurs responsables du réseau téléphonique. Grâce au financement du DoD (Department of Defence) des États-Unis, le réseau initial de commutation de paquets ARPANET[10] avait grandi au point d'inclure quatre ordinateurs en 1969. L'histoire se poursuit…

> En octobre 1972, M. Kahn a organisé une grande démonstration très réussie de l'ARPANET à la conférence ICCC (International Computer Communication Conference). C'était la première démonstration de cette nouvelle technologie de réseau auprès du public. Ce fut également en 1972 que la première application « dynamique », soit le courrier électronique, a été lancée. En mars, M. Ray Tomlinson à BBN a rédigé le logiciel de base d'écriture et d'envoi des messages électroniques, motivé en cela par la nécessité pour les développeurs d'ARPANET d'avoir un mécanisme de coordination facile[11].

Au cours des années 1970 et dans les années 1980, la plupart des réseaux informatiques étaient bâtis spécialement pour des milieux ciblés et fermés et leur usage se limitait fortement à ces milieux. Cela était vrai pour le milieu universitaire ainsi que pour le milieu commercial. Mais il y avait un désir chez les universitaires d'avoir un réseau de réseaux totalement inclusif. Le réseau britannique JANET en 1984 et le réseau américain NSFNET en 1985 ont été conçus pour être des interréseaux, le financement de la NSF (National Science Foundation) exigeant que la

---

[8] *Ibid.* à <http://www.isoc.org/internet/history/brief.shtml#Origins>.
[9] Leonard Kleinrock, « Information Flow in Large Communication Nets » *RLE Quarterly Progress Report* (juillet 1961).
[10] « (ARPANET est le sigle de Advanced Research Projects Agency Network) – Ce réseau est le précurseur d'Internet. Il a été développé vers la fin des années 1960 et le début des années 1970 par le ministère de la Défense (DoD) des États-Unis comme une expérience d'interconnexion de grands réseaux qui survivrait à une guerre nucléaire. » Voir le glossaire en ligne à <http://www.easynet.com/investorinfo/investorinfo_glossary.asp>.
[11] Cerf, *supra* note 7.

« connexion soit accessible à TOUS les utilisateurs qualifiés sur le campus »[12]. Les graines étaient semées pour l'Internet, comme nous le connaissons aujourd'hui.

Le seul ingrédient additionnel critique consistait à libérer l'Internet de sa dépendance envers l'argent public des États-Unis et donc de la restriction qui le confinait au secteur sans but lucratif de l'économie. Ce changement s'est fait graduellement au début des années 1990. En avril 1995, le financement de la NSF aux États-Unis a été retiré au réseau de base de l'Amérique du Nord. L'utilisation commerciale pleine et entière de l'Internet était permise. La fondation de l'infrastructure d'information nord-américaine était établie.

3.1.2 Développements de l'Internet au Canada

Il y a des parallèles importants entre le développement de l'interconnexion de réseaux au Canada et aux États-Unis. Nous avons la chance d'avoir une documentation étendue sur cet aspect de l'histoire récente du Canada[13]. Dans la version française, Un réseau d'un océan à l'autre, on déclare : « Ce compte rendu de l'Internet canadien nous est présenté par les personnes mêmes qui ont travaillé sur la ligne de front – les inconditionnels, les chercheurs, les innovateurs, les gens d'affaires et les politiciens[14]. »

Il y a eu un certain nombre de premiers réseaux informatiques établis par des universités canadiennes et par des entreprises canadiennes individuelles. En 1978, Bell Canada a commencé à offrir Datapac[15] qui était un réseau de données national à commutation de paquets. Ce fut l'un des premiers réseaux à commutation de paquets offert par une compagnie téléphonique au monde. Alors que Datapac utilisait la commutation de paquets, il suivait également la pratique, établie par les compagnies de téléphone, des prix en fonction du temps et de la distance. À ce moment-là, les compagnies de téléphone avaient le contrôle complet de leurs réseaux de données aussi bien que de leurs réseaux vocaux. Elles contrôlaient *tous* les appareils qui étaient directement reliés à leurs réseaux.

Les universitaires canadiens ont vite reconnu les avantages du service de transmission de messages « gratuit » utilisé par leurs collègues aux États-Unis. En 1979, le Canada se connectait à Usenet[16]. La connexion Usenet offrait une porte d'entrée dans la communauté ARPANET. Notre connexion officielle ARPANET a dû attendre jusqu'en 1983 lorsqu'un lien a été forgé avec notre propre DREnet[17]. Ce premier réseau canadien à commutation de paquets n'était pas censé être un réseau à grande échelle; il avait pour cible d'inclure au maximum une douzaine d'ordinateurs[18].

---

[12] *Ibid.*
[13] Canarie, *A Nation Goes Online – Canada's Internet History* (Montréal : Institut CA*net, 2001), en ligne : CANARIE Inc. <http://www.canarie.ca/press/publications/ango.pdf>.
[14] *Ibid.* à 5.
[15] *Ibid.* à 24.
[16] « USENET est un système mondial de groupes de discussion dont les commentaires sont transmis entre des centaines de milliers de machines. Les machines USENET ne sont pas toutes sur l'Internet. USENET est entièrement décentralisé et il a plus de 10 000 forums de discussion appelés groupes de discussion. » Voir le glossaire en ligne à <http://www.easynet.com/investorinfo/investorinfo_glossary.asp>.
[17] Canarie, *supra* notes 13 à 38.
[18] *Ibid.* à 37.

En 1984, OUnet[19] a vu le jour. Ce réseau a étendu la simple connexion entre l'Université de Waterloo et l'Université de Guelph de manière à inclure l'Université de Toronto, l'Université York, l'Université de Western Ontario, l'Université Queens, Humber College et l'Université Ryerson (Ryerson Polytechnic Institute). À mesure que ce réseau de base s'établissait, une nouvelle demande de connexion était faite par l'Université Lakehead à Thunder Bay et par trois universités en dehors de la province, soit l'Université du Manitoba, l'Université McGill et l'Université du Nouveau-Brunswick.

En une année, des plans étaient lancés pour NetNorth[20]. Le principal nœud de l'Ontario dans ce réseau plus vaste se trouvait à l'Université de Guelph. Ce serait par ce nœud que le Canada allait se connecter au réseau BITNET des États-Unis[21]. L'Université York serait l'ancre à Toronto et McGill financerait le pont avec Montréal. L'Université du Nouveau-Brunswick se connecterait par l'entremise de Montréal et assurerait, à son tour, des connexions avec l'Université de l'Île-du-Prince-Édouard et avec l'Université Mémorial à l'aide d'un pont établi à l'Université Dalhousie à Halifax. En 1989, NetNorth avait grandi au point d'inclure 65 noeuds[22].

La connexion avec BITNET était utile pour l'envoi de messages entre les chercheurs au Canada et aux États-Unis. Ce n'était pas une connexion directe avec NSFNet[23] qui était le successeur universitaire d'ARPANET. En octobre 1988, l'Université de Toronto a établi une connexion directe avec NSFNet[24]. Le Canada et NetNorth commençaient à établir la connexion avec l'interréseau américain qui deviendrait l'Internet. Ce n'était qu'une station dans la voie vers le propre CA*net du Canada. En juin 1989, le Conseil national de recherches a obtenu la permission de lancer une demande de proposition pour ce qui allait devenir CA*net[25]. En août 1990, le Conseil d'administration de CA*net recevait la nouvelle que le réseau était actif et qu'il fonctionnait avec tous les nœuds provinciaux connectés[26].

La fondation était établie. CANARIE (le sigle du Réseau canadien pour l'avancement de la recherche, de l'industrie et de l'enseignement) a été proposé en 1992[27]. La phase 1, prévue pour 1993, verrait la mise à niveau de CA*net qui passerait à une connexion T1 (1,5 Mbps ou millions de bits par seconde) dans tout le Canada. La phase suivante, qui devait se terminer en décembre 1995, devait faire une mise à niveau à T3 (45 Mbps). La phase finale devait coïncider avec la fin du siècle et voir un réseau de production entièrement mis à niveau; à ce moment-là le

---

[19] *Ibid*. à 49.
[20] *Ibid*. à 55.
[21] « (Babillard électronique) – Bitnet est un réseau informatique universitaire qui assure des services interactifs de courrier électronique et de transfert de fichiers à l'aide d'un protocole de stockage et de retransmission basé sur les protocoles Network Job Entry d'IBM. Bitnet-II encapsule le protocole Bitnet dans des paquets IP et il compte sur Internet pour leur acheminement. » Voir le glossaire en ligne à <http://www.easynet.com/investorinfo/investorinfo_glossary.asp>.
[22] *Canarie, supra* notes 13 à 58
[23] « National Science Foundation Network. La National Science Foundation a suivi le premier ARPANet en créant NSFNet en 1986 comme réseau de base à 56 Kbps pour l'Internet. » Voir en ligne : *Walt's Internet Glossary - Glossary of Internet Terms* – Lettre N <http://www.walthowe.com/glossary/n.html>.
[24] *Canarie, supra* notes 13 à 68.
[25] *Ibid*. à 92.
[26] *Ibid. à* 101.
[27] *Ibid*. à 110.

gouvernement devait se retirer du projet. La base commerciale de l'infrastructure d'information au Canada serait établie à temps pour le nouveau siècle.

3.2 Tendances générales dans le développement de la technologie

Le présent rapport est axé spécifiquement sur l'avenir de l'infrastructure d'information essentielle au Canada. Mais il y a d'importants domaines qui se chevauchent et dont il faut tenir compte afin de bien saisir notre infrastructure d'information essentielle. À un niveau général, il est utile de placer notre infrastructure d'information essentielle dans le contexte des développements technologiques auxquels nous pouvons nous attendre dans les dix prochaines années.

RAND a établi un rapport récent sur la révolution technologique mondiale intitulé *The Global Technology Revolution*[28], et sous-titré « Bio/Nano/Materials Trends and Their Synergies with Information Technology ». RAND est une institution américaine sans but lucratif qui aide à améliorer l'établissement des politiques et la prise de décision au moyen de la recherche et de l'analyse. C'est un groupe de réflexion (« Think Tank ou réservoir de pensée ») qui fait de la recherche pour les forces militaires, les services de renseignement et le service extérieur. Le premier paragraphe du sommaire donne le ton de manière utile :

> La vie en 2015 sera révolutionnée par l'effet croissant des technologies multidisciplinaires dans toutes les dimensions de la vie, dimensions sociales, économiques, politiques et personnelles. La biotechnologie nous permettra d'identifier, de comprendre, de manipuler, d'améliorer et de contrôler les organismes vivants (y compris nous-mêmes). La révolution en matière d'accessibilité et d'utilité de l'information continuera à influer profondément sur le monde dans toutes ces dimensions. Les matériaux intelligents, la fabrication rapide et la nanotechnologie changeront la façon dont nous produisons des appareils tout en élargissant leurs capacités. Ces technologies peuvent être également jointes par des « jokers » en 2015 si les obstacles à leur développement sont réglés à temps[29].

Le rapport identifie cinq métatendances clés[30]. Ces métatendances constitueront les forces fondamentales qui façonneront les développements de la technologie.

1. **Rythme accéléré du changement technologique** – Le rythme auquel les nouvelles technologies se développent continue de s'accélérer. Il y a un rythme parallèle dans l'abandon des technologies plus anciennes. La « destruction créative » qui en résulte n'est pas toujours perçue comme un élément positif par ceux qui sont directement intéressés.
2. **Nature de la technologie de plus en plus multidisciplinaire** – Les frontières entre les technologies continuent d'être floues. Ce qui est particulièrement pertinent pour l'infrastructure d'information essentielle, c'est le développement de systèmes

[28]Philip S. Anton, Richard Silberglift & James Schneider, *The Global Technology Revolution – Bio/Nano/Materials Trends and Their Synergies with Information Technology by 2015*, rapport établi pour le National Intelligence Council par RAND National Defence Research Institute, (Santa Monica : RAND, 2001) (approuvé pour publication et distribution illimitée).
[29]*Ibid.* à xi.
[30]*Ibid*. à xvi.

microélectromécanique (MEMS)[31]. Ces petits capteurs permettront de connecter tous les types d'appareils au moyen de l'infrastructure d'information.

3. **Concurrence pour le leadership en matière de développement technologique** – RAND a reconnu que le leadership en matière de développement technologique ne revient pas automatiquement à une seule nation ou à un bloc régional. L'infrastructure d'information essentielle au Canada sera façonnée par les développements réalisés ailleurs dans le monde.
4. **Mondialisation continue** – L'infrastructure d'information mondiale est une infrastructure mobilisatrice et elle est souvent un facteur de mondialisation. Nos technologies de communication et de fabrication permettent de produire des biens et services là où les coûts sont les plus bas. Ce processus est irréversible à moins d'un bouleversement social majeur.
5. **Pénétration latérale latente** – L'étude prévoit que les technologies continueront à s'infiltrer dans les zones moins développées, probablement après modification, pour les rendre plus attrayantes au niveau local.

L'étude offre un certain nombre de conclusions importantes. Un paragraphe récapitulatif fournit une description claire du monde probable à venir :

> Au-delà des révolutions agricoles et industrielles du passé, une vaste *révolution technologique* multidisciplinaire est en train de changer le monde. La technologie de l'information révolutionne déjà nos vies (particulièrement dans les pays développés) et elle continuera d'être aidée par des percées dans le domaine des matériaux et de la nanotechnologie. La biotechnologie révolutionnera les organismes vivants. Les matériaux et la nanotechnologie permettront de développer de nouveaux appareils avec des capacités imprévisibles. Non seulement ces technologies ont un impact sur nos vies, mais encore elles sont fortement imbriquées, rendant ainsi la révolution technologique fortement multidisciplinaire et accélérant les progrès dans chaque domaine[32].

L'infrastructure d'information au Canada sera l'une des clés de notre participation dans ces grands développements technologiques futurs. Il y a une importante note finale à ajouter. L'étude RAND a identifié trois « Préoccupations et Tensions »[33] qui existent déjà et qui peuvent avoir un impact croissant dans les années à venir.

1. **Disparités des classes** – Les avantages des nouvelles technologies ne se feront pas sentir de la même façon dans les régions, dans les nations et dans les classes de la société.

---

[31]« Les systèmes microélectromécaniques (MEMS ou Micro-Electro-Mechanical Systems) représentent l'intégration d'éléments mécaniques, de capteurs, d'actionneurs et de circuits électroniques sur un substrat commun de silicium au moyen de la technologie de microfabrication. Alors que les circuits électroniques sont fabriqués à l'aide de séquences de traitement de circuits intégrés (par exemple, traitement CMOS, bipolaire ou BICMOS), les composants micromécaniques sont fabriqués au moyen de processus de « micro-usinage » compatibles qui gravent sélectivement des parties de la plaquette de silicium ou qui ajoutent de nouvelles couches structurelles de manière à former les appareils mécaniques et électromécaniques. » Voir en ligne : *MEMS and Nanotechnology Clearinghouse*, « What is MEMS Technology? » (23 février 2004) <http://www.memsnet.org/mems/what-is.html>.

[32]*Ibid.* à xvii.

[33]*Ibid.*

Certains seront de véritables « gagnants » et d'autres non. Il en résultera des tensions inévitables.

2. **Protection réduite de la vie privée** – L'infrastructure d'information offrira les moyens de rendre l'information de plus en plus accessible à l'échelle mondiale. De nouvelles technologies de détection seront utilisées pour recueillir une information plus détaillée. La protection de la vie privée pourrait en souffrir.
3. **Menaces culturelles** – Le mode de vie « traditionnel » pourrait être menacé dans de nombreuses cultures par la brillante promesse des nouvelles technologies. Sans aucun doute, certains penseront que ce changement menace les valeurs culturelles de base[34].

La progression fluide des avances technologiques pourrait déraper à cause de ces préoccupations et tensions. En pensant à l'avenir, il serait bon de reconnaître que des tensions inévitables seront déclenchées par la « destruction créative » qui accompagne souvent l'introduction de technologies fondamentalement nouvelles.

3.3 Développement de la technologie de l'infrastructure d'information

Il y a quatre grands composants technologiques dans l'infrastructure d'information, soit le matériel, les logiciels, les réseaux et les services. Cette section donne un bref historique et un aperçu général des tendances probables en matière de développement dans chacun de ces domaines.

3.3.1 Développement du matériel

Une grande partie de ce qui s'est produit dans le domaine du matériel peut s'expliquer par la loi de Moore[35]. Gordon Moore est l'un des cofondateurs du géant international et fabricant de microprocesseurs Intel. En 1965, M. Moore a prédit que le nombre de transistors sur une puce doublerait tous les 12 mois. Cette prédiction hâtive était fondée sur une expérience très limitée. Avec plus d'expérience, la loi de Moore prévoit maintenant que la densité des transistors va doubler tous les deux ans environ. Cette loi a tenu pendant presque 40 ans et elle tiendra encore sans doute pendant de nombreuses années[36].

En un certain sens, la loi est devenue une prophétie auto-accomplie. Tout le monde s'attend à ce que la densité des transistors double tous les deux ans, ce qui est grossièrement traduit par « en avoir deux fois plus pour son argent tous les deux ans ». Les géants des microprocesseurs, avec Intel en tête, sont censés fournir ce genre de puissance de traitement toujours croissante. Chacun bâtit ses plans de produits d'après la loi de Moore. Il y a une pression énorme sur les fournisseurs de puces pour qu'ils soient à la hauteur de la loi. Quelles que soient les forces complexes

[34]Au moment de la rédaction de ce document, un Mennonite des États-Unis traîne au Canada, incapable pour l'instant de rentrer dans son pays natal, les États-Unis, car il n'a pas de « carte d'identité ». Selon cet homme, les préceptes de sa foi lui interdisent de transporter une « image gravée ».
[35]Gordon E. Moore, « Cramming more components onto integrated circuits » *Electronics* 38:8 (19 avril 1965), en ligne à <ftp://download.intel.com/research/silicon/moorespaper.pdf>.
[36]INTEL tient à jour une page d'information Web sur la loi de Moore; en ligne à <http://www.intel.com/research/silicon/mooreslaw.htm>.

(techniques, sociales et du marché) qui poussent les fournisseurs de puces, ils sont pratiquement sûrs que la prédiction de la loi de Moore continuera de se réaliser[37].

Cela signifie que la performance des puces s'améliore par un facteur de 1 000 tous les 20 ans. C'est devenu un facteur incroyable de changement du matériel. Cela signifie que l'ordinateur le plus puissant au monde en 1964 était devenu un ordinateur de bureau moyen en 1984 et s'est ensuite transformé en un téléphone intelligent en 2003. Dans 20 ans, cette grande puissance de traitement sera disponible dans les produits à un coût très minime; l'ère de l'ensemble « intelligent » sera arrivée.

De façon plus immédiate, on peut dire que la puissance informatique est en train de devenir un produit banalisé. De plus en plus d'ordinateurs puissants deviendront des produits standard (« off-the-shelf »). Le progrès de Dell Inc. est représentatif de ce qui se passe dans ce marché. La compagnie a été fondée par Michael Dell en 1983. Ses revenus au cours des quatre derniers trimestres s'élevaient à 41,4 milliards de dollars américains et la compagnie emploie 46 000 membres partout dans le monde[38]. Au début, Dell a vendu des ordinateurs directement au public au moyen du téléphone. La compagnie a progressé jusqu'à devenir le premier vendeur d'ordinateurs personnels au monde. Au cours des dernières années, elle ne s'est plus concentrée exclusivement sur les ordinateurs personnels et elle s'est lancée dans la vente de serveurs, d'appareils de stockage et de réseaux à de petites, moyennes, grandes et très grandes entreprises dans le monde[39].

Les ordinateurs « banalisés » et les appareils associés couvrent une gamme toujours plus grande du matériel utilisé dans des organisations de toutes tailles. Cette tendance se poursuivra sans doute. IBM offre un autre exemple qui illustre cette tendance. Lorsque Lou Gerstner a été appelé pour prendre le contrôle d'IBM en 1993, la compagnie avait vraiment des difficultés. M. Gerstner a tout d'abord commencé par couper les coûts, mais il a vite poussé la compagnie à avoir une vue de l'informatique axée sur les réseaux[40]. Son successeur, Sam Palmisano, a plutôt mis l'accent sur l'informatique « à la demande »[41]. Le but est de fournir aux clients autant de

---

[37] « Pour élargir la loi de Moore, les chercheurs d'Intel identifient et éliminent avec beaucoup de vigueur tous les obstacles qui empêcheraient la compagnie de concrétiser cette loi. En se concentrant sur les principes fondamentaux de la technologie et de la fabrication du silicium, y compris les améliorations et les innovations dans la technologie de traitement et de fabrication, dans la structure et dans les matériaux des transistors et dans l'assemblage, Intel a fait des percées au cours des deux dernières années seulement qui ont enlevé les obstacles à la continuité de la loi de Moore pendant au moins une autre décennie et sans doute au-delà. » Voir « Expanding Moore's Law – The Exponential Opportunity » *Intel Technology Update* (automne 2002), en ligne : Intel Corporation <ftp://download.intel.com/labs/eml/download/EML_opportunity.pdf>.

[38] Il y une information étendue au sujet de Dell dans son site Web (<http://www.dell.com>). En fait, la compagnie traite la plupart de ses affaires sur l'Internet. Ces faits au sujet de la compagnie se trouvent dans le site Web Dell Corporation, en ligne : http://www1.us.dell.com/content/topics/global.aspx/corp/background/en/facts?c=us&l=en&s=corp&~section=000.

[39] On peut voir la gamme des produits actuels de Dell dans la description fournie à l'intention des moyennes et grandes entreprises. Voir en ligne : <http://www1.us.dell.com/content/default.aspx?c=us&cs=555&l=en&s=biz>.

[40] Ira Sager, « The View from IBM » *Business Week* (30 octobre 1995), en ligne : Business Week Archives <http://www.businessweek.com/1995/44/b34481.htm>.

[41] « Sam Palmisano Presentation Transcript » *IBM Business Leadership Forum - San Francisco* (12 novembre 2003), en ligne : <http://www.ibm.com/ibm/sjp/11-12-2003.shtml>.

puissance informatique qu'ils le veulent, au moment et à l'endroit où cette puissance est nécessaire. La banalisation sera alors là pour de bon.

3.3.2 Développement du logiciel

Le logiciel et les langages qui servent à écrire le logiciel (langages de programmation) ont un historique riche et étendu. En 1969, Jean Sammet d'IBM a publié l'histoire « définitive » des langages de programmation[42]; il a énuméré quelque 120 langages couramment utilisés. En 1990, il était temps de publier un compendium de l'historique et des meilleurs articles sur le logiciel. Deux volumes utiles ont fait leur parution au cours de cette année[43]. Il y a toujours eu deux préoccupations constantes dans l'historique du logiciel, soit :

- **La productivité** – La loi de Moore[44] a poussé les fournisseurs de matériel à améliorer énormément les performances. Il y a eu une bataille continue pour améliorer la productivité de ceux qui développent le logiciel et en assurent la maintenance.
- **La qualité** – Les projets logiciels n'ont pas souvent atteint leurs cibles. En 1997, une étude KPMG au Canada a conclu que 61 % des produits logiciels étaient considérés comme des échecs. Des résultats semblables ont été obtenus ailleurs[45].

L'historique de la programmation décrit en détail la recherche continue de moyens toujours plus productifs de fournir du logiciel de qualité. Au cours de l'évolution des langages de programmation polyvalents, on a parlé de langages de première, de deuxième, de troisième, de quatrième et de cinquième générations. Une collection utile de définitions de termes de programmation contient une description simple des différentes générations[46] :

1. Les langages de première génération (ou 1GL) sont des langages machine peu évolués. Ce type de langage devait être optimal pour les machines; les besoins des personnes étaient rarement pris en compte.
2. Les langages de deuxième génération (ou 2GL) sont en général des langages d'assemblage qui sont également peu évolués. Ces langages étaient conçus de manière à donner un aspect convivial aux instructions machine, mais il fallait quand même une instruction du langage assembleur pour chaque instruction machine.
3. Les langages de troisième génération (ou 3GL) sont des langages évolués comme Fortran, Algol, PL/I et C. À ce stade de l'évolution, une instruction en un langage de troisième génération aurait pour résultat l'exécution de nombreuses instructions machine. Les programmeurs avaient la possibilité de dire des choses comme « prendre la valeur de A, l'ajouter à la valeur de B et mettre la somme dans C ».
4. Les langages de quatrième génération (ou 4GL) comprennent des énoncés semblables à ceux du langage humain. Les langages de quatrième génération sont couramment utilisés dans la programmation et dans les scripts des bases de données.

---

[42]Jean E. Sammet, *Programming Languages: History and Fundamentals*, (Englewood Cliffs: Prentice-Hall, 1969).
[43]Paul W. Oman & Ted G. Lewis, eds., *Milestones in Software Evolution* (Los Angeles: IEEE Computer Society Press, 1990); and Tom DeMarco & Timothy Lister, eds., *Software State-of-the-Art: Selected Papers* (New York: Dorset House Publishing, 1990).
[44]Voir la section antérieure sur la loi de Moore.
[45]Voir le taux d'échec « Failure Rate » en ligne : IT Cortex <http://www.it-cortex.com/Stat_Failure_Rate.htm>.
[46]Tiré de « Programming Definitions », en ligne : site Web Computer Hope <http://www.computerhope.com/jargon/program.htm>.

5. Les langages de cinquième génération (ou 5GL) sont des langages de programmation qui contiennent des outils visuels pour aider à développer et à représenter des programmes. Ces langages mènent à une approche entièrement visuelle de la programmation[47].

Le but ultime consiste à éliminer la nécessité de la programmation. Une fois que le programme voulu a été entièrement décrit, la traduction automatique en un logiciel d'exploitation devrait être possible. Avec l'arrivée des langages de cinquième génération, ce but se rapproche de plus en plus. Ces langages permettent aux concepteurs de logiciels de bâtir des programmes en reliant une représentation visuelle des composants standard au moyen d'une structure de flux ou de contrôle. Le diagramme *est* alors le programme. Le traducteur de langage automatique prend soin de tout ce qui est requis pour avoir un système logiciel d'exploitation complet. Cette technologie n'est pas encore largement utilisée, mais il y a déjà des systèmes 5GL qui sont offerts sur le marché[48]. On peut s'attendre à des progrès continus.

Il y a eu un certain nombre de tendances parallèles dans le développement du logiciel. Aujourd'hui, le logiciel est reconnu comme le composant qui a le plus de valeur dans de nombreux systèmes informatiques. Dans les premiers jours, le logiciel était inclus avec le matériel. Avant juin 1969, IBM « groupait » le logiciel et les services de support dans le prix de location mensuel de ses ordinateurs. IBM était le principal fournisseur d'ordinateurs. Il y avait très peu de marché pour le logiciel car le principal fournisseur donnait le logiciel qui était exécuté sur ses ordinateurs. L'opposition à cette pratique était compréhensible de la part des concurrents d'IBM. Le ministère de la Justice des États-Unis a poursuivi IBM. Après cela, en juin 1969, IBM a décidé de « dégrouper » son logiciel et ses services et de les séparer de la location du matériel[49].

L'industrie du logiciel était née. La logique était irrésistible. Si le coût de développement du logiciel pouvait être partagé entre de nombreuses organisations, les systèmes logiciels résultant devraient être supérieurs à tout ce qui pouvait être développé à l'interne. Cette brillante perspective a alimenté l'industrie du logiciel et a donné naissance à un courant continu de nouveaux produits logiciels et de nouveaux fournisseurs de logiciels. Plusieurs choses se sont produites pour transformer l'industrie du logiciel. L'ordinateur personnel est entré en scène, avec le premier ordinateur personnel d'IBM (PC) mis sur le marché en 1981[50]. Presque tout le monde

---

[47]Voir les pages de Paul Lyon en ligne : <http://www-ist.massey.ac.nz/~plyons/711_html/VPL%20papers.html>.

[48]« Cette semaine, Kinzan Inc. va sortir Kinzan Studio & Server 3.0, soit un environnement de développement et de déploiement qui permet aux développeurs de bâtir des applications d'entreprise au moyen d'un modèle d'assemblage en reliant simplement les composants avec la fonction glisser-déposer. » Voir Darryl K. Taft, « Building Java, .Net Apps Sans Coding » *EWeek-Enterprise News and Reviews* (23 février 2004) en ligne : <http://www.eweek.com/article2/0,4149,1536587,00&.asp>.

[49]Il y a beaucoup de documents sur le jugement convenu d'IBM. On peut voir un aperçu dans l'article suivant : Sara Baase, « IBM: Producer or Predator » *Reason* (avril 1974) pages 4 à 10, en ligne : <http://www-rohan.sdsu.edu/faculty/giftfire/ibm.html>.

[50]« Le modèle PC 5150 d'IBM a été annoncé à une conférence de presse à New York le 12 août 1981 et il a été mis sur le marché au début de l'automne 1981. C'est cet ordinateur, tel qu'il a été fabriqué par IBM et sous forme de clone, qui est devenu la norme de facto des entreprises pendant le reste de la décennie et au-delà. Le modèle de base se détaillait à 2 880 $ et comprenait 64 kilo-octets de mémoire RAM et un lecteur de disquette 5,25" simple face de 160 kilo-octets. L'ajout d'un lecteur de disque dur ou l'augmentation de la mémoire pouvait faire augmenter le prix considérablement. Le PC d'IBM était alimenté par un processeur Intel 8088 de 3,77 MHz. » Voir « 1981: The IBM

commençait à utiliser le PC d'IBM ou son clone comme poste de travail personnel. Il y a eu une véritable explosion de fournisseurs qui offraient des logiciels pour le nouveau PC. En deux décennies, Microsoft avait réussi à dominer le marché du logiciel de PC. Selon une étude récente, le système d'exploitation Windows de Microsoft a presque 98 % de la part[51] du marché des systèmes d'exploitation de bureau.

En même temps que Microsoft gagnait une position dominante dans le marché du logiciel de bureau, le marché des applications logicielles d'entreprise subissait également un changement important. Peut-être que le changement le plus important était celui du degré de planification et d'installation des applications d'entreprise vers la fin du siècle dernier. L'intégration était essentielle au succès de ces activités pilotées par le logiciel. Et l'intégration entre les produits d'un seul fournisseur de logiciels est presque toujours plus facile à réaliser que l'intégration entre des applications provenant de différents fournisseurs. C'est presque une vérité de La Palice dans le marché des applications d'entreprise. Le fournisseur allemand du logiciel SAP[52] est le leader dans les applications intégrées à l'échelle de l'entreprise. Et le fournisseur californien de bases de données Oracle[53] est le leader en matière d'applications bâties à partir d'une base de données partagée.

Toutefois, la nature du marché de ces grandes applications logicielles est assez différente de celle du marché du logiciel de bureau. Dans le logiciel de bureau, il y a un seul fournisseur dominant. Dans le domaine des applications d'entreprise, le marché suit le modèle plus traditionnel du fournisseur principal qui a deux fois la part du marché du deuxième fournisseur, celui-ci ayant deux fois la part du marché du troisième, ce qui laisse alors une minuscule part du marché pour tous les autres fournisseurs. Bien entendu, les principaux fournisseurs aimeraient que le marché des applications logicielles d'entreprise suive la direction prise par le marché du logiciel de bureau. Les récentes visées d'Oracle sur PeopleSoft[54] ne sont que l'une des actions les plus visibles pour renforcer la position de tête du fournisseur sur le marché.

Il y a un facteur additionnel dont il faut tenir compte au sujet du développement du logiciel et c'est la tendance croissante envers l'adoption du logiciel de source ouverte (« logiciel libre »). Des développeurs consacrent gratuitement du temps et de l'énergie à bâtir du logiciel. Le logiciel résultant est mis gracieusement à la disposition de tous ceux qui veulent l'utiliser. Le système d'exploitation Linux[55] est maintenant la fondation reconnue des applications de source ouverte. On peut donner au moins deux facteurs importants pour expliquer l'enthousiasme des particuliers et des organisations en faveur du logiciel de source ouverte :

Personal Computer is Introduced » *CED in the History of Media Technology*, en ligne : site Web CED Magic <http://www.cedmagic.com/history/ibm-pc-5150.html>.

[51]Voir « Microsoft's Windows OS global market share is more than 97% according to OneStat.com » (10 septembre 2002), en ligne : <http://www.onestat.com/html/aboutus_pressbox10.html>.

[52]Voir « SAP Info », en ligne : SAP INFO <http://www.sap.info/en/>.

[53]Voir en ligne : site Web Oracle <http://www.oracle.com/>.

[54]Voir Lisa Vaas, « PeopleSoft, You Will Be Assimilated » *EWeek-Enterprise News and Reviews* (5 février 2004), en ligne : <http://www.eweek.com/article2/0,4149,1517233,00.asp>.

[55]Voir Ragib Hasan, « History of Linux », en ligne : <https://netfiles.uiuc.edu/rhasan/linux/> pour avoir le point de vue d'un initié sur l'historique de Linux.

- **La fierté du mordu de l'informatique** – Il est clair que bien des personnes qui contribuent aux applications de source ouverte sont motivées par la fierté et l'enthousiasme envers leurs réalisations professionnelles. Ce sont des « hackers »[56] et fiers de l'être. Cela ne fait pas de mal non plus que des contributions de source ouverte reconnues et bien formées paraissent très bien dans un curriculum vitæ.
- **Les services de vente –** Un certain nombre de compagnies de source ouverte ont été fondées en suivant le principe de donner le logiciel de base et de vendre ensuite les services pour rendre l'utilisation de ce logiciel plus facile. Red Hat[57] est l'un des premiers exemples parmi les plus réussis. IBM[58] s'est positionnée comme une compagnie qui offre du support d'entreprise pour le logiciel de source ouverte.

Il est important d'ajouter une mise en garde au sujet de Linux. SCO[59] a poursuivi IBM, alléguant que IBM avait fait incorporer illégalement dans Linux[60] du code qui appartenait à SCO (ou à ses prédécesseurs). SCO a également poursuivi des utilisateurs de Linux. Si jamais SCO gagnait, ce serait un véritable coup dur pour Linux. Dans ce cas, l'avenir du logiciel de source ouverte serait sérieusement assombri.

En ce qui concerne le matériel, on peut faire en toute confiance de bonnes prédictions au sujet de ses capacités futures. Dans le cas du logiciel, l'avenir est beaucoup moins clair. Toutefois, nous pouvons sûrement prédire que la « crise » du logiciel se poursuivra. Wikipedia en ligne offre l'explication suivante[61] :

> La notion d'une crise du logiciel a vu le jour à la fin des années 1960. Une première utilisation du terme se trouve dans la conférence de Edsger Dijkstra (« The Humble Programmer ») donnée en 1972 au Prix ACM Turing et publiée dans les Communications de l'ACM. M. Dijkstra déclare : « [la principale cause de la crise du logiciel est] que les machines sont devenues plus puissantes de plusieurs ordres de grandeur! Disons-le carrément : tant qu'il n'y avait pas de machines, la programmation ne posait aucune difficulté; lorsque nous avons eu quelques faibles ordinateurs, la programmation est devenue un problème moyen et maintenant que nous avons des ordinateurs gigantesques, la programmation est devenue également un problème gigantesque. »

Même si toutes les brillantes promesses des langages de programmation de la cinquième génération se matérialisent, nous devrons quand même faire face à une « crise » du logiciel. Le problème est que le logiciel d'entreprise réussi doit être bâti selon un modèle réussi pour l'entreprise que le logiciel dessert. Si l'auteur du logiciel ne comprend pas le problème de

---

[56]Voir « Hack, Hackers, and Hacking », en ligne : Jesper / Laisen / DK <http://www.laisen.dk/Hack__Hackers__and_H.1233.0.html>.
[57]Voir en ligne : Red Hat, Inc. <http://www.redhat.com/>.
[58]Voir « Linux at IBM », en ligne : IBM Corp. <http://www-1.ibm.com/linux/>.
[59]Voir en ligne : Le groupe SCO <http://www.sco.com>.
[60]Voir « Linux & Open Source », *EWeek-Enterprise News and Reviews*, en ligne : < http://www.eweek.com/category2/0,4148,1237915,00.asp> pour avoir une couverture continue du conflit dans ce domaine.
[61]Voir « Software Crisis », *Wikipedia, the free encyclopedia,* en ligne : Wikipedia.org <http://en.wikipedia.org/wiki/Software_crisis>.

l'entreprise, il est fort peu probable que le programme résultant soit réussi. L'acquisition de la connaissance nécessaire du domaine[62] exigera toujours beaucoup de travail.

Au-delà de cette « prédiction », nous pouvons soulever quelques questions.

> **Question :** La domination de Microsoft dans le monde de la bureautique se poursuivra-t-elle?
>
> Microsoft détient actuellement plus de 95 % du marché du logiciel de bureau. Windows est le système d'exploitation dominant et Office est l'application de bureau dominante. Des questions ont été soulevées au sujet des répercussions de cela sur la sécurité de notre infrastructure d'information[63]. La tendance à adopter Linux dans le bureau peut être envisagée comme une correction « naturelle » de l'état actuel « anormal » du marché du logiciel de bureau.
>
> **Question :** La domination de Microsoft en bureautique se traduira-t-elle en domination dans d'autres domaines (par exemple, les serveurs, les appareils portatifs et/ou les produits de consommation)?
>
> De nombreux faits attestent que Microsoft aimerait dominer le marché des systèmes d'exploitation dans différents secteurs – la compagnie a lancé un certain nombre de systèmes d'exploitation connexes qui peuvent être exécutés dans plusieurs plates-formes différentes. Mais la domination de Microsoft en bureautique ne s'est pas répétée dans d'autres marchés… pas encore. Microsoft a un historique qui prouve que la compagnie finit toujours par avoir les produits qu'il faut[64]. La compagnie trouvera-t-elle ce qu'il faut pour les autres plates-formes?
>
> **Question :** Est-ce que la connaissance de l'« ingénierie logicielle » va se développer, fleurir et être couramment appliquée?
>
> L'expression « ingénierie logicielle » (« software engineering ») a été inventée pour les Conférences du Comité scientifique de l'OTAN qui ont eu lieu en 1968 et en 1969; « l'expression « ingénierie logicielle » a été délibérément choisie pour son côté provocateur qui implique la nécessité d'adopter dans la fabrication du logiciel les types de fondations théoriques et de disciplines pratiques qui sont traditionnels dans les

---

[62]« SANS UNE CONNAISSANCE D'EXPERT d'un problème particulier, il est évident que l'on ne peut établir des algorithmes complexes (comme ceux du supercalculateur Deep Blue) ni essayer de trouver une solution à un problème particulier. La rapidité, la puissance, le logiciel de l'ordinateur ou les algorithmes ne résolvent pas le problème à eux seuls. Si on ne comprend pas bien la question à régler, « rouler plus rapidement » n'est tout simplement qu'un autre moyen de tourner à vide. » Voir IBM Deep Computing Institute, en ligne : IBM Corporation <http://www.research.ibm.com/dci/cat4_domain.shtml>.

[63]Dan Geer *et al*. « Cyber*In*security: The Cost of Monopoly – How the Dominance of Microsoft's Products Poses a Risk to Security » (27 septembre 2003), en ligne : Computer & Communications Industry Association <http://www.ccianet.org/papers/cyberinsecurity.pdf>.

[64]On a observé officieusement qu'à la troisième version d'un produit, Microsoft arrive à savoir ce qu'il faut faire exactement. Cela s'est produit avec Windows 3.0 et avec Internet Explorer 3.0. Si on lui laisse suffisamment de temps, Microsoft peut souvent trouver ce qu'il faut faire pour avoir du succès.

branches établies de l'ingénierie.[65] ». En 30 années, ce titre « provocateur » s'est transformé en ce que bien des gens appelaient la « véritable » ingénierie logicielle[66]. Combien de temps faudra-t-il attendre avant d'avoir vraiment une ingénierie du logiciel?

Question : Est-ce que le logiciel canadien fera partie des domaines de pratique réservés?

Le Canada a une caractéristique inhabituelle en ce sens que de nombreux domaines traditionnels de l'ingénierie entrent dans ce que nous appelons des domaines de pratique réservés. Étant donné la façon dont le génie (ingénierie) est réglementé dans la plupart des provinces canadiennes, on peut soutenir qu'un certain type de pratique dans le domaine du logiciel ne devrait être exécuté que par ceux qui détiennent la licence ou l'autorisation d'exercer appropriée. La Vision stratégique 2001 de l'Ordre des ingénieurs de l'Ontario soulève exactement ce point[67]. S'il peut y avoir ingénierie du logiciel et que des ingénieurs avec licence savent comment exécuter ce genre d'ingénierie, cela milite fortement en faveur de la licence[68].

3.3.3 Développement des réseaux

Par le passé, plusieurs options étaient offertes pour l'utilisation des réseaux au Canada. De plus en plus, les réseaux IP (Internet Protocol) sont le choix dominant. C'est certainement vrai dans le cas des réseaux qui sont exclusivement utilisés pour le transport des données. Les réseaux vocaux ont suivi un chemin différent, mais cela est en train de changer. Le protocole VoIP (Voice over Internet Protocol) est aujourd'hui une option intéressante pour les organisations plus importantes[69] et Rogers Communications Inc.[70] prévoit l'offrir aux consommateurs en 2005. De plus en plus, les réseaux de tous genres suivront le protocole IP. Les réseaux canadiens ne seront

---

[65]J. M. Buxton, Peter Naur, & Brian Randell, eds., *Software Engineering: Concepts and Techniques*, (New York Petrocelli/Charter, 1976) à 6.

[66]Les deux plus grandes sociétés professionnelles dans le domaine des technologies de l'information aux États-Unis, soit ACM et IEEE-CS, ont étudié la question de savoir si l'ingénierie logicielle a avancé au point de devenir une véritable profession. Les deux sociétés n'étaient pas d'accord, mais elles ont continué à travailler ensemble sur les développements dans le domaine. Voir « History of the Joint IEEE Computer Society and ACM Steering Committee for the Establishment of Software Engineering as a Profession », en ligne : IEEE Computer Society <http://www.computer.org/tab/seprof/history.htm>.

[67]Est-ce que la profession d'ingénieur veut « jouer un rôle de leadership proactif dans des domaines additionnels de pratique réservés, soit les sciences appliquées et la technologie, ou veut-elle simplement attendre et réagir aux propositions qui seront établies? » En appuyant cette motion, George Comrie a noté que la réglementation qui protège l'intérêt public dans des domaines non réglementés comme le développement du logiciel sera sans doute établie à l'avenir. « La question, dit-il, est de savoir si nous voulons être proactifs ou réactifs. Nous pouvons nous opposer après le fait ou nous pouvons intervenir dès le départ. » Voir Connie Mucklestone, « Strategic Plan Vision sparks lively discussion », réunion du 26 mars 2001, en ligne : Professional Engineers Ontario (Ordre des ingénieurs de l'Ontario) <http://www.peo.on.ca/publications/DIMENSIONS/mayjune2001/MJ01InCouncil.pdf>.

[68]Il y a fort peu d'unanimité sur cette question dans le domaine du logiciel. Robert Fabian a présenté l'argument contraire dans *ComputerWorld Canada*, en ligne : <http://www.fabian.ca/profper/pp9.html>.

[69]L'organisation à laquelle les auteurs de ce rapport sont affiliés, Gowling Lafleur Henderson LLP, a déployé la technologie VoIP pour les communications dans tous ses bureaux au Canada.

[70]« Ted Rogers, président-directeur général, a déclaré hier à la conférence UBS Warburg que la compagnie de Toronto allait commencer un service téléphonique au moyen de la technologie Internet. » Voir Mark Evans, « Rogers Edges Toward Telephony War v. BCE 'Prudent For Us': Will Start Service Using Internet By 2005, Says CEO » *National Post* (10 décembre 2003), en ligne : <http://www.vonage.com/corporate/press_news.php?PR=2003_12_10_1>.

pas tous interconnectés, mais ils suivront le développement des réseaux IP. L'Internet est le « grand-père » de tous les réseaux IP (c'est véritablement un réseau de réseaux ou un interréseau).

Il y a un grand nombre de tendances qui façonneront l'avenir de l'Internet. Dans cette section, nous identifierons quelques-unes de ces tendances clés. Le rythme auquel les changements se produiront dépendra de nombreux facteurs. Quelques-uns des principaux facteurs s'appliqueront à l'extérieur du Canada – les États-Unis auront un impact important sur l'avenir de l'Internet tel qu'il est perçu par les Canadiens et dans les institutions canadiennes. Un bon nombre de ces facteurs déterminants pourraient interagir de façon imprévisible et, bien qu'il soit téméraire d'offrir une seule prédiction assurée de l'avenir d'Internet, il est quand même possible d'esquisser une gamme de possibilités pour l'avenir.

3.3.3.1 Rapidité

Il y a eu une augmentation constante de la rapidité des réseaux. En 1968, les principaux ordinateurs du réseau qui était le précurseur de l'Internet étaient interconnectés au moyen de liaisons de 50 kbps (milliers de bits par seconde). C'était considéré comme un débit rapide. En quelques années, les utilisateurs étaient connectés à ces ordinateurs à l'aide de modems rapides de 2,8 kbps. Il y a dix ans, une connexion rapide à domicile utilisait un modem commuté de 56 kbps. Aujourd'hui, une connexion rapide à domicile utilise une liaison à large bande de 1 000 kbps. Nous nous rapprochons rapidement du moment où la vidéo de grande qualité sera transmise par cette connexion à domicile. La rapidité des interconnexions commerciales a augmenté en parallèle.

Comme il a été mentionné, la loi de Moore sur les semi-conducteurs déclare que la puissance des puces double tous les 18 à 24 mois. Nous avons vu une augmentation continue de la puissance informatique car il y a une série continue de nouvelles puces. Une tendance semblable peut être observée dans les réseaux, mais les sauts se font par étapes plus discrètes (par exemple, d'un modem commuté de 56 kbps à un modem câble ou DSL (ligne d'abonné numérique) de 1 000 kbps). Ce qui montre une croissance continue, c'est la vitesse moyenne de connexion. Cette vitesse moyenne a suivi le rythme de la loi de Moore et elle continuera sans doute à suivre ce rythme avec les progrès dans le domaine des semi-conducteurs. Cette pensée mène à la prédiction qu'en dix ans une connexion rapide de téléphone cellulaire pourra supporter la vidéo bidirectionnelle de grande qualité.

3.3.3.2 Sans fil

De plus en plus d'appareils utiliseront une connexion réseau sans fil. Cette tendance se remarque déjà dans l'utilisation croissante du téléphone cellulaire. Vous pouvez également la voir dans votre café local où une connexion Internet sans fil est offerte gratuitement ou à faibles coûts avec votre boisson préférée. Vous pouvez aussi voir en partie cette tendance dans le nouveau service d'aide sans fil qui est fourni, à un prix mensuel modique, à de nombreux propriétaires de voiture. Vous pouvez également la voir dans la conception de nouveaux bureaux sans fil où les ordinateurs doivent être branchés pour avoir l'électricité, mais non pour obtenir une connexion réseau. Le sans fil est en train de croître rapidement, même dans les zones de villégiature.

Cette tendance envers le sans fil change les rôles dont on peut s'acquitter au moyen d'une connexion réseau. Ce sera bientôt chose commune que de retrouver des articles et des personnes

grâce à leur connexion avec le réseau. Une série de nouvelles questions est soulevée par cette tendance envers le sans fil. Les personnes pourront-elles avoir des connexions Internet anonymes et, plus précisément, des connexions sans fil qui ne permettent pas de les localiser? Il y a aussi des questions importantes au sujet de la priorité qui doit être donnée aux services dans les signaux de diffusion publics utilisés par les appareils sans fil – est-ce que l'appel d'un adolescent (qui se sent seul) à un ami peut bloquer le signal d'une ambulance?

3.3.3.3 Appareils connectés

Aujourd'hui, le détaillant Wal-Mart est en train d'essayer des cartons qui viennent équipés d'appareils radiofréquences à courte distance. Chaque carton dans l'entrepôt peut être repéré par sa connexion sans fil à courte distance. Le coût est assez faible pour faire cela avec des milliers de cartons par semaine, mais encore bien trop élevé pour que cette méthode soit adoptée partout. Mais attendez que la loi de Moore se mette de la partie. En quelques années, le coût de cette connexion à faible portée sera vraiment minime. Quelques années après cela, une connexion complète au réseau mondial coûtera aussi une misère. À ce stade, il serait réaliste de donner à « tout ce qui est » important une connexion réseau.

3.3.3.4 Réseau unique

Actuellement, on utilise souvent des réseaux distincts pour la voix, le câble, les données et l'accès Internet. Mais des services comme la voix sur Internet (VoIP) sont en rapide croissance. Et de plus en plus de connexions de données sont faites « virtuellement » à l'aide de l'Internet mondial (avec des connexions au réseau privé virtuel). Fait important, c'est presque en train de devenir une question purement économique. L'établissement d'un « canal » d'information virtuel entre deux points sur l'Internet coûte de moins en moins cher et offre de plus en plus de fonctions. Au cours des dix prochaines années, les réseaux distincts deviendront de moins en moins essentiels, ils se rétréciront au point de ne plus pouvoir offrir des services réseau concurrentiels. À mesure que cela se produit, l'Internet mondial jouera un rôle de plus en plus dominant. Ce sera de moins en moins pratique d'utiliser des réseaux de rechange. Les répercussions sur la façon dont les services de l'infrastructure d'information essentielle sont assurés pourraient être graves.

3.3.3.5 Pourriel

Aujourd'hui, il y a un problème croissant avec le pourriel (spam), c'est-à-dire le courriel de masse non sollicité. On a estimé que plus de la moitié du trafic actuel de messagerie électronique sur l'Internet est du pourriel. Dans le cas de ceux qui ont des adresses électroniques « populaires », il est courant de trouver que 90 % du courrier d'arrivée, ou plus, est du pourriel. Les forces économiques sont en faveur du pourriel de façon écrasante. Cela ne coûte presque rien d'envoyer des centaines de milliers de messages qui sont des pourriels. Avec un taux de participation aussi faible que 0,001 %, c'est encore très intéressant sur le plan économique d'envoyer des pourriels. À notre avis, cela ne peut pas continuer[71]. Il faut faire quelque chose à ce sujet et bien des remèdes auront des répercussions sérieuses sur la façon dont l'infrastructure d'information essentielle du Canada sera pourvue.

[71]Voir Garrett Hardin, « The Tragedy of the Commons » *Science* 162 (1968): 1243-1248, en ligne : <http://www.dieoff.com/page95.htm>.

3.3.3.6 Protocoles

Le premier réseau de recherche avant l'Internet visait à accommoder jusqu'à 256 réseaux informatiques distincts. À ce moment-là, personne ne pensait qu'il allait falloir connecter des millions et des millions d'ordinateurs. Très vite, toutefois, la limite a dû être augmentée. Le protocole Internet actuel (IPv4) a été conçu de façon à permettre à quatre milliards d'appareils distincts d'avoir leurs propres adresses Internet. Cela peut sembler être un grand nombre d'adresses, mais diverses considérations techniques limitent fortement la façon dont de nombreuses adresses « libres » sont offertes pour utilisation aux nouveaux appareils qui veulent se connecter à l'Internet. On se demandait sérieusement si l'Internet allait manquer d'adresses pour tous les appareils qui voulaient se connecter.

Une proposition a été déposée pendant un certain nombre d'années pour remplacer le protocole Internet actuel (IPv4) par une nouvelle version améliorée (IPv6). Le nouveau protocole Internet (version 6)[72] augmenterait de façon très importante le nombre d'adresses Internet disponibles. Mais la conversion de la version 4 à la version 6 serait coûteuse et difficile. Un certain nombre de solutions de rechange techniques ont été établies. Bon nombre de ces solutions ont été conçues pour permettre à plusieurs appareils ayant un point de connexion réseau (appelé un routeur) de partager une adresse. Nous avons « manqué » de nouvelles adresses Internet pendant plusieurs années, mais les solutions de rechange permettent à l'Internet de continuer à croître.

La principale motivation derrière IPv6 était d'augmenter l'espace adresse, mais cela fournirait aussi des avantages additionnels importants. Particulièrement dans le cas de la connexion avec l'infrastructure d'information essentielle du Canada, la nouvelle version IPv6 permettrait d'établir l'ordre de priorité des paquets de messages. Les paquets « importants » auraient un plus grand nombre des ressources réseau disponibles. Les messages critiques pourraient être acheminés dans le réseau même si le réseau était « encombré » par du trafic peu important. Est-ce que le protocole IPv6 deviendra la norme? Le Canada devrait-il installer IPv6, ou un protocole amélioré semblable, dans les principaux éléments de l'infrastructure d'information essentielle?

3.3.4 Développement des services TI

Depuis les tout premiers jours dans ce domaine, les organisations ont compris la valeur de l'informatique. Il n'est pas étonnant que ce besoin ait inspiré des fournisseurs qui ont alors développé et offert les *services des technologies de l'information (TI)* dans ce marché. Ces services étaient fondés sur ce que le fournisseur espérait être une combinaison attrayante et profitable de matériel, de logiciels et de connectivité (réseaux). Dans les années 1950 et 1960, il était courant de trouver des « fournisseurs » qui offraient du temps de location dans leurs ordinateurs. De nombreux centres informatiques universitaires ont trouvé que c'était un moyen intéressant de compléter leurs revenus.

---

[72] « Cette série de pages Web donne de l'information au sujet de la version 6 du protocole Internet (IPv6). Le protocole IPv6 est parfois aussi appelé le protocole Internet de la prochaine génération ou IPng. IPv6 a été recommandé par les directeurs régionaux IPng du Groupe d'étude sur l'ingénierie Internet (IETF) à la réunion IETF qui a eu lieu à Toronto le 25 juillet 1994, dans le document RFC 1752 intitulé *The Recommendation for the IP Next Generation Protocol*. La recommandation a été approuvée par le groupe directeur de l'ingénierie Internet et c'est devenu un projet de norme le 17 novembre 1993. » Voir en ligne : Sun Microsystems, Inc. – Internet Engineering group of Solaris Software <http://playground.sun.com/pub/ipng/html/ipng-main.html>.

Dans les années 1970, il y avait un marché florissant de sociétés de services informatiques au Canada. C'était au moment où les gros ordinateurs étaient très coûteux à acheter et à exploiter. Des économies d'échelle pouvaient être réalisées. Les compagnies groupaient leurs besoins informatiques afin de pouvoir acheter conjointement les plus gros ordinateurs centraux. Plusieurs universités canadiennes ont adopté une approche semblable. Pendant une certaine période, on pouvait faire véritablement des économies grâce à l'utilisation partagée des plus gros ordinateurs possibles.

Dans les années 1980 et 1990, le marché des services TI a changé de nouveau. Avec le lancement des ordinateurs personnels et la croissance de la puissance des mini-ordinateurs, les avantages des économies d'échelle dans le cas des gros ordinateurs étaient réduits. Les sociétés de services se sont alors concentrées sur des services plus spécialisés. En 1985, l'Université de Toronto s'est lancée dans le domaine des superordinateurs, offrant des cycles sur son superordinateur Cray[73]. Un certain nombre de firmes ont commencé à offrir des services de traitement de la paie[74]. Le marché des cycles de traitement dans de gros ordinateurs polyvalents a continué à rétrécir. Les fournisseurs de services TI qui restaient sur le marché se sont concentrés sur des services spécialisés.

En ce début du 21e siècle, le marché des services TI change de nouveau. Une gamme croissante de services TI est offerte par l'entremise d'Internet ou au moyen de fonctions de communications plus spécialisées. La gestion des relations avec la clientèle (CRM ou Customer Relationship Management)[75] est actuellement une application populaire. Une vaste gamme de systèmes logiciels est offerte aux compagnies qui peuvent alors les installer sur leurs propres ordinateurs. Il y a également un marché croissant pour des services CRM fournis par l'Internet[76]. Ce qui est nouveau dans ces services en ligne, c'est qu'ils s'imbriquent dans la structure de l'organisme client, c'est-à-dire que tous ceux qui « touchent » un client utiliseront le service CRM en ligne (à distance).

Nous voyons également une énorme croissance dans le domaine de l'externalisation (outsourcing)[77]. En fait, l'externalisation peut prendre de nombreuses formes. Ce qui est particulièrement intéressant pour le sujet global traité dans le présent rapport, c'est la tendance vers l'externalisation à l'extérieur du pays lorsque le travail TI est expédié à des fournisseurs étrangers à moindres coûts (ou à qualité supérieure). L'une des prédictions récentes est que cette forme d'externalisation des TI s'élèvera de 16 milliards de dollars en 2004 à 46 milliards de dollars en 2007 aux États-Unis[78]. On peut s'attendre à des changements semblables au Canada, même si nous pouvons tirer avantage de la valeur inférieure de notre dollar et recevoir ainsi des travaux TI à exécuter pour les États-Unis.

---

[73]Voir en ligne : University of Toronto Press <http://www.utppublishing.com/uoft_history/notes/notes_chapter39.pdf>.
[74]Voir en ligne : ADP Canada <http://www.adp.ca/en/index.html> qui est un chef de file sur le marché canadien actuel de l'impartition.
[75]Pour avoir de l'information générale au sujet de la gestion des relations avec la clientèle, voir en ligne le centre de recherche Customer Relationship Management Research Center <http://www.cio.com/research/crm>.
[76]Salesforce.com, en ligne :<http://www.salesforce.com/> est l'un des chefs de file dans ce domaine.
[77]Voir en ligne : <http://www.outsourcing.com/> pour de l'information générale au sujet de l'externalisation.
[78]Voir en ligne : site Web CIO – Metrics <http://www2.cio.com/metrics/2004/metric667.html>.

Les organisations ont toujours acheté quelques-uns des services dont elles avaient besoin pour fonctionner. Ce qui est nouveau, c'est que nous voyons une dépendance croissante en temps réel par rapport aux fournisseurs de services qui sont en dehors de l'organisation. Cette tendance semble se poursuivre. On commence à peine à aborder les questions de responsabilité.

3.4 Calendrier prévu pour l'infrastructure d'information

Un certain nombre d'études[79] ont été entreprises pour prévoir l'avenir de l'infrastructure d'information en Amérique du Nord, en Europe et ailleurs. Un rapport[80] qui a été établi pour l'établissement américain Institute for Information Infrastructure Protection[81] comprend un calendrier utile. Il présente une projection sur l'infrastructure d'information avec des prévisions pour 2006, 2010 et 2020. Même si cela a été établi précisément pour les États-Unis, la plupart des prévisions peuvent fort bien s'appliquer à l'infrastructure d'information du Canada. Le reste de cette section comprend notre version corrigée de ce calendrier.

3.4.1 Caractéristiques prévues de l'infrastructure d'information à court terme (2006)

- Les divers composants de l'infrastructure TI (appareils de poche, ordinateurs portatifs, ordinateurs de bureau, gros ordinateurs, serveurs et applications existantes) continueront d'être difficiles à intégrer et d'avoir des problèmes de stabilité.
- Les capteurs et les microprocesseurs intégrés commenceront à exécuter une grande variété de fonctions, particulièrement dans le contrôle des processus. Les cartes intelligentes commenceront à être utilisées.
- Des réseaux spécifiques d'entreprise auront des frontières qui seront de plus en plus mal définies. Ce sera dû en partie à l'utilisation d'appareils qui peuvent être partout (par exemple, communications sans fil, informatique mobile et technologies d'agent mobile). Ce sera dû aussi en partie aux collaborations dynamiques entre les organisations.
- Les particuliers utiliseront des quantités croissantes de technologies de l'information. Cela inclura l'utilisation d'assistants numériques personnels (PDA) et la fourniture du contenu selon la position (au moyen de dispositifs GPS et de téléphones cellulaires). Il y aura également le recours accru à la convergence des médias numériques et à l'intégration de la voix, des données, des images fixes et de la vidéo.
- L'infrastructure des télécommunications de base continuera à être câblée et basée de plus en plus sur IP. L'adoption du sans fil augmentera de façon importante avec les communications à grande portée (par satellite), les communications locales (Bluetooth et WiFi) et cellulaires (2.5G et 3G).

---

[79] Anton, Silberglitt, & Schneider, *supra* note 28; Robert H. Anderson *et al*., *The Global Course of the Information Revolution: Technological Trends: Proceedings of an International Conference*, (Santa Monica: RAND, 2001); *Technology Timeline*, BTexact Technologies (division de British Telecommunications) (novembre 2001), en ligne : <http://www.btexact.com/docimages/42270/42270.pdf>.

[80] *National Information Infrastructure Protection Research and Development Agenda Initiative Report*, Institute for Information Infrastructure Protection, (9 septembre 2002), en ligne : <http://www.thei3p.org/documents/analyses/I3P_Roadmap_Analysis_V1.0s.pdf> [*Initiative Report*].

[81] Voir en ligne : <http://www.thei3p.org/index.php>.

3.4.2 Caractéristiques prévues de l'infrastructure d'information à moyen terme (2010)

- L'utilisation de capteurs intégrés sera courante dans les applications personnelles et souvent transparente pour les utilisateurs (par exemple, les moniteurs de santé portables qui font partie intégrante des vêtements de « support »).
- Les entreprises dépendront de plus en plus de la technologie de localisation (GPS ou autres) pour suivre les entités physiques importantes pour l'organisation.
- Les frontières entre les réseaux, les appareils et les formats (voix, données, vidéo, contrôle, etc.) seront floues et les distinctions entre les fournisseurs et entre les fournisseurs et les utilisateurs se réduiront. Les contrôles traditionnels de réglementation seront de moins en moins efficaces.
- La collaboration au moyen de l'infrastructure d'information se répandra de plus en plus et elle s'intégrera à la façon dont les groupes sociaux, les équipes de travail et les organisations fonctionnent. Les connexions seront dynamiques, reliant tous et chacun n'importe où dans les communautés.
- Les capacités de réseau s'étendront de façon importante. Les débits des données sans fil se compareront aux débits des données de bureau d'aujourd'hui (plus de 5 Mbps). La vidéo en continu et la voix sur IP (VoIP) seront courantes. De véritables progrès seront réalisés dans l'adoption du protocole IPv6.

3.4.3 Caractéristiques prévues de l'infrastructure d'information à long terme (2020)

- Dans les sociétés développées, pratiquement tout ce qui est important pourra se connecter au réseau. La distinction entre des objets physiques importants et des entités cybernétiques deviendra plus floue.
- La technologie du sans fil couvrira presque toute l'Amérique du Nord et fournira un débit fiable en térabits aux entreprises et toutes les capacités vidéo aux particuliers.
- La nanotechnologie sera commercialement disponible et elle commencera à être utilisée partout.
- La loi de Moore tiendra toujours, peut-être grâce à l'informatique quantique, donnant aux appareils de poche les capacités de la superinformatique.

Le rapport où ces prévisions ont été établies[82] comprend également des prévisions sur les caractéristiques de la sécurité de l'information en 2006, en 2010 et en 2020. Ces prévisions en matière de sécurité[83] sont en dehors de la portée de cette section, mais elles peuvent être utiles lorsqu'on envisage différents modèles de responsabilité.

[82] *Initiative Report, supra* note 81.

[83] *Ibid*. page 46. Ce document prévoit « qu'il y aura un corps évolué de règles juridiques sur la sécurité de l'information qui sont fondées sur la législation et sur les affaires judiciaires » et « que les questions de sécurité de l'information seront une considération normale …, tout comme le sont aujourd'hui les questions de sécurité physique ». Ces prévisions en matière de sécurité peuvent être jugées trop optimistes.

3.5 Développement de l'infrastructure d'information essentielle

Il y a eu une tendance forte et omniprésente dans les organisations canadiennes à remplacer le dicton traditionnel « des hommes, de l'argent et du matériel » par une meilleure information. Tout le mouvement « juste à temps » ou « fabrication sans gaspillage » peut être vu comme un mouvement qui ne fait rien d'autre que remplacer les stocks régulateurs qui caractérisaient anciennement la fabrication par une meilleure information. La motivation évidente est que l'information coûte moins que « les hommes, l'argent et le matériel » qui sont remplacés.

Les répercussions de cette tendance sur l'infrastructure d'information essentielle au Canada seront importantes. Le Canada a déjà identifié ses secteurs d'infrastructure essentiels[84]. En plus du Secteur des communications, qui comprend l'infrastructure de l'information, il y a neuf autres secteurs essentiels. Pour tous ces secteurs, l'information a servi à remplacer « les hommes, l'argent et le matériel ». Les dix secteurs sont décrits dans la table 3.1.

Table 3.1 Infrastructures essentielles du Canada

Secteur	Exemples de sous-secteurs cibles
1. Énergie et services publics	Énergie électrique (production, transmission, énergie nucléaire) Gaz naturel Systèmes de production et de transmission du pétrole
2. Communications	Télécommunications (services satellitaires, téléphoniques et par câble) Systèmes de diffusion Réseaux (Internet)
3. Finances	Services bancaires Valeurs Investissements
4. Soins de santé	Hôpitaux Établissements de santé Établissements de distribution des produits sanguins Laboratoires Services pharmaceutiques
5. Secteur alimentaire	Sécurité alimentaire Secteur agricole et alimentaire Distribution des produits alimentaires
6. Eau	Eau potable Gestion des eaux usées
7. Transports	Transport aérien Transport ferroviaire Transport maritime Transport de surface

[84]Bureau de la protection des infrastructures essentielles et de la protection civile, *An Assessment of Canada's National Critical Infrastructure Sectors* (juillet 2003), en ligne : Sécurité publique et Protection civile Canada <http://www.psepc-sppcc.gc.ca>.

Secteur	Exemples de sous-secteurs cibles
8. Sécurité	Sécurité chimique, biologique, radiologique et nucléaire Matières dangereuses Recherche et sauvetage Services d'urgence (services de police, d'incendie, d'ambulance et autres services d'urgence) Barrages
9. Gouvernement	Installations gouvernementales Services gouvernementaux (par exemple, les services météorologiques) Réseaux d'information du gouvernement Biens gouvernementaux Principaux symboles nationaux (institutions culturelles et lieux et monuments historiques)
10. Secteur manufacturier	Industrie chimique Base industrielle de défense

L'infrastructure d'information au Canada joue un rôle essentiel dans le fonctionnement continu et en douceur de tous ces secteurs. L'impact d'une défaillance de notre infrastructure d'information pourrait varier. Les principaux symboles nationaux continueraient d'être ouverts et accessibles au public, mais le filtrage en ligne des visiteurs en vue d'identifier des menaces possibles à la sécurité serait éliminé tout comme le traitement en ligne des frais d'entrée. En ce qui concerne notre réseau électrique, l'infrastructure d'information du Canada est essentielle à notre capacité d'équilibrer la charge entre différents sous-réseaux et différentes sources de production. Une panne rapide serait sans doute due à une défaillance de notre infrastructure d'information.

Aujourd'hui, de nombreux secteurs d'infrastructure essentiels continueraient à fonctionner de façon limitée même en cas de panne majeure de notre infrastructure d'information. À mesure que la technologie progresse, le fonctionnement continu possible face à la défaillance de l'infrastructure d'information deviendra de plus en plus limité. Notre infrastructure d'information est en train de devenir rapidement *le* principal moteur du fonctionnement continu de tous les autres secteurs d'infrastructure essentiels.

4.0 Introduction à la responsabilité

4.1 Qu'est-ce que la responsabilité?

Même si cette section du rapport peut sembler quelque peu technique sur le plan juridique, son importance deviendra apparente dans les sections ultérieures.

Afin de traiter du rôle que la responsabilité joue ou pourrait jouer dans l'infrastructure d'information essentielle, il est utile de mieux saisir ce que signifie le terme responsabilité.

Dans le sens général du dictionnaire, « la responsabilité » signifie être responsable de ses actions (voir « accountability »[85]). À son tour, « responsable » signifie « quelqu'un qui doit rendre compte (à une personne ou à une chose)[86]. À partir de là, on peut déduire que toute définition de la « responsabilité » doit spécifier, au moins, qui doit rendre compte à qui et de quoi.

Selon l'approche traditionnelle, les questions ou éléments suivants devraient au moins être traités dans les analyses ultérieures. Étant donné le rythme de changement de l'infrastructure d'information, il peut y avoir aussi des éléments dynamiques additionnels dont il faut tenir compte.

4.1.1 Responsable de quoi

À notre avis, la responsabilité fonctionne le mieux lorsqu'il y a des définitions claires et sans ambiguïté des obligations assumées par les participants (ou qui leur sont imposées) dans l'infrastructure d'information essentielle et pour lesquelles une personne ou une organisation sera tenue responsable. Ces obligations pourraient être établies par les sources habituelles, y compris par une combinaison de contrats, de droit de la responsabilité délictuelle et des obligations légales. Par exemple, afin de justifier l'attribution de responsabilités aux participants qui sont des fournisseurs de services pour leurs actes ou omissions, ces obligations devraient comprendre des descriptions clairement définies des services à fournir ainsi que les niveaux auxquels ces services doivent être fournis.

4.1.2 Qui est responsable

Les principes utilisés dans l'attribution des responsabilités aux acteurs d'un réseau, comme l'Internet, ont fait l'objet d'exposés antérieurs[87]. En citant le principe de Varian-Anderson[88] [89], Yahalom note que la responsabilité devrait être attribuée de manière à s'assurer que « ceux qui sont le plus en mesure de contrôler les risques ont les stimulants appropriés à cet effet » et, en

---

[85]The Oxford Encyclopaedic English Dictionary, 2d ed., *s.v.* « accountability ».
[86]*Ibid.*
[87]Raphael Yahalom, « Liability Transfers in Network Exchanges », article publié pour l'atelier Workshop on Economics and Information Security qui a eu lieu à l'University of California, Berkeley, les 16 et 17 mai 2002, en ligne : UC Berkeley, <http://www.sims.berkeley.edu/resources/affiliates/workshops>.
[88]Ross Anderson, « Why Information Security is Hard – An Economic Perspective », (Proceedings of the 17th Computer Security Applications Conference, New Orleans, Louisiana, Dec. 2001), en ligne : Annual Computer Security Applications Conference <http://www.acsac.org/2001/papers/110.pdf>.
[89]Hal R. Varian, « Managing On-Line Security Risks », Economic Science Column, *The New York Times*, (1er juin 2000), en ligne : The New York Times, <http://www.nytimes.com/library/financial/columns/060100econscene.html>.

citant Anderson[90], Yahalom note que « lorsque la partie qui est en mesure de protéger un système n'est pas la partie qui subirait les résultats des défaillances en matière de sécurité, il faut alors s'attendre à avoir des problèmes ».

Yahalom[91] soutient que l'on peut étendre ces principes de manière à attribuer la responsabilité aux parties qui sont bien en mesure de perpétrer certains événements malveillants et qui ont des stimulants à cet effet.

Dans certains cas, l'attribution des responsabilités entre les parties sera assumée par accord mutuel en vertu d'un contrat. Dans d'autres cas, l'attribution des responsabilités pourrait être imposée aux parties selon les obligations établies dans le droit de la responsabilité délictuelle ou dans les obligations légales.

4.1.3 Envers qui être responsable et exécution de la loi

Lorsqu'il y a des problèmes dans le fonctionnement de l'infrastructure d'information essentielle parce que l'un ou plusieurs des participants n'ont pas rempli leurs obligations, la source de l'obligation déterminera les demandeurs éventuels. C'est-à-dire que la partie publique et la partie privée pourraient demander réparation pour les pertes ou les dommages subis à la suite de violations de contrat ou de manquements aux obligations légales ou aux responsabilités délictuelles.

4.1.4 Capacité de mesure

Afin de pouvoir attribuer les responsabilités entre les parties pour les problèmes dus au fonctionnement de l'infrastructure d'information essentielle, il faut pouvoir surveiller et mesurer, à un degré approprié de précision, les actes ou les omissions de toutes les parties intéressées.

Toutefois, la complexité structurelle et l'interdépendance de fonctionnement entre les éléments qui constituent l'infrastructure d'information essentielle font de l'exécution de ces tâches un exercice non négligeable. De la même façon, cette complexité et cette interdépendance gênent également les décisions en matière de causalité, d'éloignement et autres moyens traditionnels d'attribuer, de mesurer et d'évaluer les dommages.

4.1.5 Conséquences des violations

En même temps que les obligations elles-mêmes, il faut également bien comprendre les conséquences du manquement à s'acquitter de ces obligations, y compris les recours possibles pour ceux qui ont subi des préjudices ou des pertes à cause d'un tel manquement.

[90] Anderson, *supra* note 88.
[91] Yahalom, *supra* note 87.

4.2 Nécessité de comprendre la structure et la dynamique de l'infrastructure d'information essentielle

Le présent document vise à faire comprendre le rôle que la responsabilité doit, peut et pourrait jouer dans le développement et dans le fonctionnement de l'infrastructure d'information essentielle. Pour cela, il est important de saisir le cadre global de responsabilité dans lequel l'infrastructure d'information essentielle s'est développée et fonctionne, aujourd'hui et probablement à l'avenir. Cela englobe la compréhension des éléments publics au Canada et à l'échelle internationale (par exemple, les lois, règlements, politiques et mécanismes d'exécution appropriés) ainsi que les éléments du secteur privé au Canada et à l'échelle internationale (par exemple la structure et la dynamique des marchés des biens et services qui sont produits pour les participants de l'infrastructure d'information essentielle et qui sont utilisés par ces participants).

Sans une solide compréhension de l'infrastructure d'information essentielle globale et de la dynamique de son développement, les décisions qui sont prises dans le secteur privé et dans le secteur public risquent de ne pas avoir les effets prévus. Pire encore, les effets d'actes bien intentionnés du secteur public et du secteur privé peuvent donner des résultats indésirables. Il faut une recherche approfondie pour bâtir la solide compréhension requise.

Voici quelques-unes des questions qu'il faut se poser pour avoir une meilleure compréhension de toute l'infrastructure d'information essentielle et du rôle de la responsabilité dans cette infrastructure :

1. Comment le niveau ou l'attribution des responsabilités entre les participants dans l'infrastructure d'information essentielle touchent-ils le développement et le fonctionnement de l'infrastructure d'information essentielle?
2. De quelles façons la responsabilité a-t-elle contribué à un état souhaitable, ou indésirable, de l'infrastructure d'information essentielle?
3. Quels attributs décrivent le mieux l'infrastructure d'information essentielle actuelle et future et quelles sont les mesures correspondantes?
4. Quelle est la recherche actuelle au sujet de chacun de ces attributs et que faudrait-il savoir d'autre?
5. Comment et de quelle façon l'état futur voulu de l'infrastructure d'information essentielle est-il lié à chacun des attributs?
6. Quelles sont les relations entre les divers attributs pertinents de l'infrastructure d'information essentielle et quelles sont les solutions de compromis entre eux?
7. Quelles sont les relations, y compris les solutions de compromis, entre les divers attributs de l'infrastructure d'information essentielle et les politiques qui les gouvernent?

5.0 Objectifs de la responsabilité dans le domaine de l'infrastructure d'information essentielle

La section 4 de ce rapport introduit brièvement la notion de responsabilité. Dans cette section, nous explorons la façon dont la responsabilité peut s'appliquer à l'infrastructure d'information essentielle. Nous pensons que le meilleur point de départ dans cet exercice est de considérer nos objectifs. Des objectifs clairs, établis dès le départ, constituent la base qui nous permet de garder le cap et de corriger la trajectoire au besoin.

5.1 Objectifs selon la perspective adoptée

Les différents participants dans le domaine de l'infrastructure d'information essentielle ont différents objectifs. Tout le monde s'entend généralement pour dire que nous dépendons de plus en plus de l'infrastructure d'information essentielle et que nous devons nous assurer qu'elle continue de fonctionner. Au-delà de ce point toutefois, on semble fort peu s'entendre sur ce qui doit être fait, le cas échéant.

Il vaut mieux commencer l'exercice d'identification des objectifs à partir d'une base de référence. D'abord et avant tout, il nous semble que la société canadienne veut continuer à fonctionner. À notre avis, le Canada veut également prospérer et croître en tant que nation. En même temps, il est extrêmement important d'assurer la sécurité de tous ses membres.

Pour remplir ces objectifs, les infrastructures essentielles (indiquées dans la table 3.1) doivent fournir des fonctionnalités fiables et évolutives. Comme il est mentionné dans la section 3.5, ces infrastructures essentielles comptent de plus en plus sur l'infrastructure d'information essentielle. Ainsi, la société requiert que l'infrastructure d'information essentielle continue de fournir le soutien voulu aux autres infrastructures essentielles. Jusque-là, tout va bien. Mais vient ensuite la première question difficile : comment allons-nous assurer que l'infrastructure d'information essentielle fournit les prestations voulues?

5.2 Diversité et responsabilité : les deux points influents

Au cours de notre recherche, de nombreux participants clés ont mentionné deux facteurs dont il fallait tirer parti pour assurer une infrastructure d'information essentielle fonctionnelle et solide, soit la diversité et la responsabilité. Bien des personnes estimaient que, dans un monde parfait, nous aurions une infrastructure d'information essentielle composée d'un certain nombre de composants divers, mais fonctionnellement équivalents, à chacun des niveaux. Cela était souvent accompagné du souhait que nous aurions des responsabilités claires et significatives pour tous les aspects de l'infrastructure. Cela nous donnerait deux mécanismes distincts de sûreté intégrée. Dans le monde réel, il y a des difficultés à atteindre la diversité et des niveaux élevés de responsabilité. Non seulement cela, mais la diversité et la responsabilité ne se séparent pas facilement; elles interagissent entre elles. À notre avis, nous devons nous efforcer de choisir la solution la plus raisonnable pour chacun de ces points.

5.2.1 Diversité

Les Canadiens ne sont pas étrangers à la diversité. En fait, notre pays est bâti sur la diversité. Nous comprenons les défis et les avantages mieux que tout autre pays au monde. En profondeur, nous savons que les organisations sociales sont plus solides lorsqu'elles ont un degré élevé de diversité interne car elles peuvent exploiter cette diversité pour répondre aux menaces externes.

Selon l'un des points de vue, l'infrastructure d'information essentielle est un ensemble de parties qui communiquent et travaillent ensemble dans un but commun. Il y a donc de puissants parallèles entre l'infrastructure d'information essentielle et une organisation sociale. Une infrastructure d'information essentielle qui comprend une diversité de composants à chaque niveau a au moins un certain niveau de redondance. Par exemple, prenons le cas de deux réseaux de base distincts avec des composants clés de l'infrastructure d'information essentielle connectés aux deux réseaux. Si l'un des réseaux tombe en panne, l'autre absorbera une partie du trafic.

L'idée d'utiliser la diversité pour bâtir un réseau fiable a servi de fondement à la première idée de réseau qui a mené à l'Internet. L'article fondamental de Paul Baran qui a paru en 1964 exprime précisément cette idée[92].

La section 5.3 décrit la façon dont la diversité interagit avec la responsabilité. La section 5.5 traite des moyens avec lesquels le gouvernement peut encourager la diversité dans l'infrastructure d'information essentielle.

5.2.2 Responsabilité : processus ou résultats

5.2.2.1 Responsabilité en matière de résultats

Un bon nombre de nos idées au sujet de la responsabilité ont vu le jour à un moment où les choses étaient plus simples. Vous ne pouviez avoir votre service téléphonique (service local, interurbain et équipement) qu'auprès d'un seul fournisseur. Il en était de même pour l'électricité. Les ordinateurs, dans la mesure où ils existaient, n'étaient connectés qu'à des terminaux dans un seul bâtiment. Dans ces scénarios, on pensait fort peu à la responsabilité et, en fait, cela ne méritait pas plus. Si le service téléphonique ou le réseau électrique tombait en panne, on savait fort bien qui était responsable. Les niveaux de complexité, particulièrement dans le domaine de la technologie de l'information, ont augmenté de plusieurs ordres de grandeur. Les modèles de responsabilité n'ont pas suivi ce rythme.

La responsabilité dans le domaine de l'infrastructure d'information essentielle peut paraître faussement simple de prime abord. L'infrastructure d'information essentielle est, de par sa nature même, essentielle (critique); elle doit fonctionner. Par conséquent, les gens pensent généralement que si nous tenons les opérateurs de l'infrastructure d'information essentielle responsables de ce fonctionnement, nous aurons fait beaucoup de chemin pour assurer ce fonctionnement. Malheureusement, ici comme dans de nombreuses autres situations, « la difficulté réside dans l'application pratique ».

---

[92]Paul Baran, « On Distributed Communications » The Rand Corporation (août 1964), en ligne : Rand Corporation <http://www.rand.org/publications/RM/RM3420/index.html>.

Lorsque nous envisageons la responsabilité de cette façon, nous le faisons dans le sens traditionnel, comme il est décrit ci-dessus pour le service téléphonique et le réseau électrique. On tient les gens ou les organisations responsables des résultats. À part les questions de sécurité, nous n'étions pas trop préoccupés par la façon dont les résultats étaient obtenus. C'était logique. Le principe de responsabilité/d'autorité était maintenu. (Plus simplement, ce principe énonce qu'il n'est pas raisonnable de tenir quelqu'un responsable de quelque chose à moins qu'il n'ait l'autorité sur cette chose.) Malheureusement, ce type de responsabilité a une applicabilité limitée dans l'infrastructure d'information essentielle.

Il est important de comprendre que l'infrastructure d'information essentielle n'est pas une chose. C'est plutôt un groupe partiellement défini d'appareils, de liaisons, de données, de services et d'organisations que nous avons assez subjectivement mis ensemble dans un même panier. Il y a de nombreuses interdépendances. Les services essentiels fournis par l'infrastructure d'information dépendent en général d'un certain nombre de fournisseurs qui travaillent conjointement. Il y a à la fois des dépendances directes et des dépendances indirectes. Dans ces conditions, il devient rapidement presque impossible de tenir les gens responsables de la prestation d'un genre quelconque de fonctionnalités de haut niveau. Il y a trop de choses que ces personnes ne contrôlent pas.

La responsabilité en matière de résultats a du sens aux niveaux de granularité plus raffinés de l'infrastructure d'information essentielle. Les « résultats » peuvent inclure non seulement la fonctionnalité fournie, mais aussi d'autres éléments comme le niveau de sécurité. Des normes peuvent être établies. La norme ISO 17799, traitée dans la section 9.4.4, en est un bon exemple.

5.2.2.2 Responsabilité en matière de processus

Heureusement, il y a un autre type de responsabilité et c'est celui de la responsabilité en matière de processus. Les disciplines professionnelles nous en fournissent des exemples excellents. Les vérificateurs ne sont pas responsables de l'exactitude des états financiers vérifiés de la compagnie. Ils ont la responsabilité de mener une vérification selon les normes généralement acceptées et de donner leur opinion, fondée sur leur vérification, au sujet de l'exactitude des états financiers.

À notre avis, la responsabilité en matière de processus peut s'appliquer fortement à l'infrastructure d'information essentielle. Les pratiques appropriées en architecture et méthodologie nous permettent de bâtir des systèmes fiables à partir de composants non fiables. La responsabilité en matière de processus nous permet de définir la façon dont les liaisons et les nœuds clés de l'infrastructure d'information essentielle sont testés et certifiés. Finalement, elle peut aider à spécifier le code de conduite, les niveaux de connaissance et les domaines de pratique des professionnels qui travaillent dans l'infrastructure d'information essentielle.

5.3 Interaction entre la diversité et la responsabilité

Au début de cette section, nous avons signalé que la diversité et la responsabilité ne se séparent pas facilement, En fait, la responsabilité peut parfois offrir une solution de rechange à la diversité. Par exemple, il y a des occasions où nous, en tant que société, choisissons un monopole réglementé de préférence à une diversité concurrentielle. Dans ce sens, il y a un équilibre à atteindre. Il n'est peut-être pas nécessaire d'avoir des niveaux élevés de responsabilité s'il y a une diversité suffisante. Il y a toutefois une interaction qui peut être beaucoup plus importante entre la responsabilité et la diversité.

La responsabilité peut fonctionner avec la diversité pour créer une infrastructure d'information essentielle plus solide. Pour expliquer cela, continuons avec notre exemple de la section 5.2.1 où nous avions deux réseaux de base indépendants avec des composants individuels de l'infrastructure d'information essentielle connectés aux deux réseaux. Du trafic essentiel est acheminé par chacun des réseaux. Le protocole IPv6, qui avait été traité dans la section 3.3.3.6, offre la possibilité de spécifier la qualité de service d'un paquet dans l'en-tête. Si nous définissons les composants individuels de l'infrastructure d'information essentielle, nous pouvons utiliser IPv6 pour donner à tout le trafic entre ces composants la priorité la plus élevée. Ainsi, si jamais il y a une panne dans l'un des réseaux de base, tout le trafic essentiel du réseau en panne exigera d'avoir la priorité dans le réseau en fonctionnement. Il n'y aura donc presque pas d'interruption dans l'infrastructure d'information essentielle; en d'autres termes, la redondance sera presque complète, sans l'exigence habituelle en matière de capacité disponible. C'est une adaptation du concept qui a été proposé pour gouverner l'interaction entre les communications à bande étroite et les communications à bande ultra-large[93].

5.4 Solutions d'équilibre et de compromis

Dans le monde réel, les solutions de compromis sont inévitables. Le succès se traduit par l'atteinte du bon équilibre. Voici quelques solutions importantes de compromis qui influent sur l'infrastructure d'information essentielle :

- Le coût par rapport à la disponibilité
- Le coût par rapport à la fonctionnalité
- Les préoccupations nationales par rapport aux pressions internationales
- L'ordre du jour du fournisseur par rapport à celui de l'utilisateur
- La perspective d'ensemble par rapport à l'aspect pratique
- Le temps de mise en œuvre par rapport à la durée de vie utile.

[93]Kevin D. Werbach, « Supercommons: Toward a Unified Theory of Wireless Communication », en ligne : Social Science Research Network Electronic Library <http://papers.ssrn.com/sol3/delivery.cfm/delivery.cfm/SSRN_ID456020_code031013670.pdf?abstractid=456020>.

6.0 Principaux participants

Cette section identifie les principaux groupes de participants et traite de leurs fonctions dans l'infrastructure d'information.

6.1 Gouvernement

Les organismes du secteur public ont un impact important sur la mise en forme de l'infrastructure d'information. Ils exercent également une influence importante dans le domaine de la responsabilité. Les sous-sections suivantes indiquent les groupes du secteur public qui exercent directement ces influences. Le gouvernement qui est l'un des principaux utilisateurs de l'infrastructure d'information essentielle est traité dans la section 6.3.

6.1.1 Organismes de réglementation/législateurs

Ce groupe comprend les établissements gouvernementaux qui s'occupent essentiellement de l'administration, de la réglementation, de l'octroi des licences et de l'inspection de l'infrastructure d'information essentielle; le groupe inclut aussi ceux qui établissent les politiques et les lois.

Comme exemples de participants, citons les ministères fédéraux suivants, ainsi que les organismes provinciaux ou municipaux correspondants :

- Parlement
- Ministère de la Justice
- Bureau du Conseil privé
- Conseil du Trésor
- Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC)
- Conseil canadien des normes

6.1.2 Sécurité et protection

Ce groupe s'occupe directement de la sécurité et de l'intégrité de l'infrastructure d'information essentielle. Comme exemples de participants, citons les ministères fédéraux suivants, ainsi que les organismes provinciaux ou municipaux correspondants :

- Sécurité publique et Protection civile Canada (SPPCC)
- Ministère de la Défense nationale (MDN)
- Centre de la sécurité des télécommunications (CST)
- Industrie Canada

6.1.3 Fournisseurs de programmes

L'une des façons dont le gouvernement influence l'infrastructure d'information est celle de la stimulation économique directe et indirecte. Comme exemples de participants, citons les ministères fédéraux suivants, ainsi que les organismes provinciaux ou municipaux correspondants :

- Industrie Canada
- Infrastructures Canada

6.2 Associations

Les associations sont des participants importants de l'infrastructure d'information essentielle au Canada car elles servent souvent à regrouper les opinions et les préoccupations de leurs membres.

6.2.1 Associations professionnelles

Les membres des associations professionnelles comprennent des personnes qui travaillent dans les autres groupes clés de participants. Ces associations ont pour but de faire avancer les professions qu'elles représentent et de promouvoir les intérêts professionnels de leurs membres. Ces associations sont classifiées selon le code SCIAN (NAICS) – 813920 des organisations professionnelles. Le code SCIAN est traité dans la section 6.4.1 ci-dessous. Voici des exemples d'associations professionnelles canadiennes :

- Association canadienne de l'informatique (ACI/CIPS) www.cips.ca
- Association of Internet Marketing and Sales (AIMS) www.aimscanada.com

6.2.2 Normes

Les normes qui portent sur l'infrastructure d'information essentielle au Canada sont établies à la fois par des organisations nationales et internationales. En voici des exemples :

- Institute of Electrical and Electronics Engineers (IEEE) www.ieee.org
- Agence canadienne d'enregistrement Internet (ACEI/CIRA) www.cira.ca
- Internet Corporation For Assigned Names and Numbers (ICANN) www.icann.org
- Association canadienne de normalisation (ACNOR/CSA) www.csa.ca

6.2.3 Fournisseurs

Il y a un certain nombre d'associations qui représentent les fournisseurs de produits et services de l'infrastructure d'information essentielle au Canada. En voici quelques-unes :

- Association canadienne de la technologie de l'information (ACTI/ITAC) www.itac.ca.
- Association canadienne des télécommunications sans fil (ACTS/CWTA) www.cwta.ca

Ces associations sont classifiées selon le Système de classification des industries de l'Amérique du Nord (SCIAN/NAICS), code 813910 – Associations d'affaires. Le système SCIAN est traité dans la section 6.4.1. Outre la promotion des intérêts commerciaux de leurs membres, ces associations peuvent « mener des recherches sur les nouveaux produits et services, publier des bulletins, établir des statistiques sur le marché ou parrainer des normes de qualité et de certification »[94].

[94]Statistique Canada, *Système de classification des industries de l'Amérique du Nord (North American Industry Classification) (NAICS) 2002*, en ligne : Statistique Canada, <http://stds.statcan.ca/english/naics/2002/naics02-class-search.asp?criteria=813910>.

6.3 Utilisateurs

L'infrastructure d'information essentielle au Canada est définie comme l'infrastructure d'information qui soutient les dix infrastructures essentielles définies par SPPCC[95]. Celles-ci ont été récapitulées à la table 3.1.

Les utilisateurs qui sont les principaux participants de l'infrastructure d'information essentielle sont les organisations qui comprennent ces secteurs essentiels. Dans la plupart des cas, ces organisations pourraient bien être représentées par les dirigeants principaux de l'information (DPI/CIO) pour leurs dépendances par rapport à l'infrastructure d'information essentielle.

6.4 Fournisseurs

6.4.1 Aperçu

Une grande communauté de fournisseurs offrent et/ou exploitent les composants de l'infrastructure d'information. Ces fournisseurs se divisent en quatre groupes selon l'activité économique : logiciels, matériel, réseaux et services. Même si de nombreuses compagnies chevauchent les catégories, cette segmentation est malgré tout très utile car chaque catégorie a des préoccupations, des produits et des mécanismes de responsabilité distincts et reconnaissables. En outre, comme la plupart des produits sont vendus « dégroupés », les compagnies qui chevauchent ces catégories ont en général des divisions internes distinctes qui s'occupent de chacune des catégories.

Afin de préciser les organisations qui se trouvent dans chacune des quatre catégories, nous avons choisi de classer les catégories selon le Système de classification des industries de l'Amérique du Nord (SCIAN/NAICS). C'est un système de classification standard qui a remplacé l'ancien système de 1980 appelé Classification type des industries (CTI/SIC). Le SCIAN[96] a été développé conjointement par Statistique Canada, par l'ECPC (Economic Classification Policy Committee) des États-Unis et par l'INEGI (Instituto Nacional de Estadística, Geografía e Informática) du Mexique. La table de correspondance du SCIAN pourrait se révéler utile s'il fallait une base de sondage pour les recherches ultérieures.

[95] *An Assessment of Canada's National Critical Infrastructure Sectors*, Bureau de la protection des infrastructures essentielles et de la protection civile, juillet 2003.

[96] Vous trouverez plus d'information sur le SCIAN (NAICS) à l'adresse : http://www.statcan.ca/english/Subjects/Standard/naics/2002/naics02-index.htm.

Table 6.1 Table de correspondance SCIAN

Catégorie	N° SCIAN	Description
Logiciel	511210	Éditeurs de logiciels
Matériel	334110	Fabrication d'ordinateurs et d'équipement périphérique
	334210	Fabrication des appareils téléphoniques
	334220	Fabrication de l'équipement de radiodiffusion et de télévision ainsi que des communications sans fil
	334410	Fabrication des semi-conducteurs et d'autres composants électroniques
	335920	Fabrication des fils et des câbles de communications et d'électricité
Communications/ Services réseau	517110	Entreprises de télécommunications avec fil
	517210	Entreprises de télécommunications sans fil (à l'exception des satellites)
	517310	Revendeurs dans le domaine des télécommunications
	517410	Télécommunications par satellite
	517510	Distribution par câble et par d'autres programmes
	517910	Autres télécommunications
	518110	Fournisseurs de services Internet, portails de recherche Web
	518210	Traitement des données, hébergement et services connexes
Consultations et services	541510	Conception des systèmes informatiques et services connexes
	811210	Réparation et entretien de l'équipement électronique et de précision
	611420	Formation en informatique
	237130	Construction des lignes d'électricité et de communications et structures connexes

6.4.2 Logiciel

Les fournisseurs ou éditeurs de logiciels sont définis par Statistique Canada comme suit[97] :

> « Cette classe canadienne comprend les établissements dont l'activité principale est l'édition de logiciels, habituellement pour de nombreux clients et habituellement désignés par l'expression logiciels de série. Les établissements de cette classe exécutent les opérations nécessaires à la production et à la distribution de logiciels telles que la conception, la fourniture de la documentation, l'assistance en matière d'installation et la prestation de services de soutien aux acheteurs de logiciels. Ces établissements peuvent se livrer à la conception et à l'édition, ou se consacrer uniquement à l'édition. »

Ces fournisseurs offrent le logiciel système qui permet d'exploiter la plus grande partie de l'infrastructure d'information essentielle ainsi que le logiciel d'application qui fournit la plupart des fonctionnalités de l'infrastructure d'information essentielle.

6.4.3 Matériel

Les fournisseurs du matériel sont des compagnies qui fabriquent et vendent le matériel des ordinateurs et des communications qui est utilisé dans l'infrastructure d'information essentielle. Cela comprend des éléments comme les ordinateurs, les périphériques, les routeurs et les commutateurs.

6.4.4 Communications/Services réseau

La principale fonction de ce groupe est d'exploiter le réseau qui est la fondation de l'infrastructure d'information essentielle.

6.4.5 Consultations et services

Cette catégorie comprend les firmes qui s'occupent de la conception, de la construction et de la maintenance de l'infrastructure d'information essentielle. La table 3.1 donne une certaine indication des types de firmes auxquels on a recours.

En voici quelques exemples :

- Développement personnalisé de programmes informatiques
- Services de gestion des installations TI
- Développement de sites Web
- Firmes de consultants en intégration de systèmes

---

[97] Statistique Canada, *Système de classification des industries de l'Amérique du Nord (SCIAN) (North American Industry Classification NAICS) 2002*, en ligne : Statistique Canada, <http://stds.statcan.ca/english/naics/2002/naics02-class-search.asp?criteria=511210>. (Note du traducteur : La citation en français est tirée du site Web de Statistique Canada.)

6.5 Observateurs de l'industrie

L'infrastructure d'information essentielle est importante, complexe et changeante. Cela a donné lieu au développement d'un grand nombre de firmes dont les activités comprennent le suivi, l'analyse et les rapports sur l'industrie. Ces firmes aident à garder tous les autres participants au courant des développements pertinents et leurs opinions exercent souvent une influence importante sur les orientations dans le domaine et sur les fortunes des organisations individuelles.

Ces observateurs (ou services de veille) comprennent une vaste gamme de firmes, mais les firmes qui ont un impact important sur l'infrastructure d'information essentielle se divisent généralement en organisations de médias TI et de chercheurs.

Les activités des organisations de médias qui se concentrent sur les technologies de l'information (TI) englobent les publications spécialisées, les publications destinées aux consommateurs et les foires commerciales. Elles peuvent être à la fois canadiennes et internationales. En voici des exemples :

- ComputerWorld, www.computerworld.com
- PC Magazine, www.pcmag.com
- eWeek, www.eweek.com
- Real World Linux Conference and Expo, www.realworldlinux.com

Quant aux chercheurs, on les retrouve dans des firmes spécialisées dans les étude de marché TI ainsi que dans les universités et au gouvernement. Voici quelques exemples d'entreprises qui se spécialisent dans les études de marché TI :

- IDC Canada, www.idc.ca
- Gartner, www.gartner.com
- Meta Group, www.metagroup.com

7.0 Responsabilité dans d'autres environnements

7.1 Introduction

Le défi d'avoir le « bon » niveau de responsabilité dans le cas des infrastructures essentielles est universel. Il chevauche à la fois les autres infrastructures essentielles et d'autres juridictions. De nombreuses leçons ont été apprises (essentiellement à la suite d'erreurs). Nous croyons qu'un certain nombre de ces leçons tirées d'autres environnements ont de la pertinence pour ce qui est de la responsabilité dans le domaine de l'infrastructure d'information essentielle. Il nous vient à l'esprit cette pensée de Confucius : « Nous pouvons apprendre la sagesse par trois méthodes : premièrement, par la réflexion, ce qui est le plus noble; deuxièmement, par l'imitation, ce qui est le plus facile et troisièmement, par l'expérience, ce qui est le plus amer. » Dans ce rapport, nous allons essayer les deux premières méthodes.

Les parties suivantes donnent de brefs résumés de la façon dont la responsabilité est traitée dans d'autres environnements. Nous avons sélectionné ces exemples car nous estimons que les leçons en matière de responsabilité ont une pertinence particulière pour l'infrastructure d'information essentielle. Nous traitons de cette pertinence dans la dernière partie.

7.2 Professionnels de la santé

7.2.1 Historique du concept de responsabilité

Historiquement, la réglementation moderne dans les professions de la santé a commencé vers la fin du 19e siècle et au début du 20e siècle avec l'émergence de la réglementation d'État dans la médecine. Afin d'éviter les risques associés à une « pratique médicale dangereuse », les gouvernements ont promulgué des lois pour réglementer les praticiens dans le domaine des soins de santé. Le groupe des médecins a été le premier à obtenir avec succès un tel contrôle sanctionné par l'État. L'évolution ultérieure des régimes de réglementation des fournisseurs de soins de santé a suivi un modèle qui avait été conçu pour réglementer la médecine et qui était fondé sur une définition juridique générale de la portée de la pratique de la médecine[98].

La Constitution[99] accorde aux provinces et aux territoires le pouvoir de réglementer les professions. Les gouvernements provinciaux et territoriaux ont, à leur tour, édicté des lois qui délèguent le pouvoir de réglementation des diverses professions à des organisations composées des membres de ces professions. Ces organismes professionnels de réglementation sont généralement autoréglementés dans les limites de leur pouvoir légal et on leur a accordé le droit

[98] Douglas Alderson & Deanne Montesano, *Regulating, De-regulating and Changing Scopes of Practice in the Health Professions – A Jurisdictional Review* (rapport établi pour le Conseil consultatif de réglementation des professions de la santé (CCRPS/HPRAC) (avril 2003) à 3, en ligne : Health Professions Regulatory Advisory Council <http://www.oaccpp.on.ca/news/appendix1-dp.pdf>.

[99] *Constitution Act, 1867* (U.K.), 30 & 31 Vict., c.3, réimprimé dans R.S.C. 1985, App. II, No. 5.

à l'autoréglementation afin qu'ils puissent remplir leur mandat qui est de protéger et de promouvoir l'intérêt du public[100].

À mesure que les soins de santé se sont développés et ont évolué au Canada, il y a eu une augmentation constante du nombre de professions autoréglementées (l'autoréglementation des médecins et des dentistes remonte à la Confédération). Il y a eu une croissance extrêmement rapide dans le nombre de professions de la santé au cours des années 1960 et 1970 à cause de l'émergence de diverses sous-spécialités. Actuellement, il y a plus de 35 professions de la santé qui sont réglementées au Canada, l'approche prédominante étant celle de l'autoréglementation. En général, l'autoréglementation a évolué historiquement à cause des lois, à la suite de l'acceptation ou de la reconnaissance de ce principe par les principaux acteurs dans le secteur des soins de santé (sur le plan économique et politique)[101].

Un exemple qui illustre ce point est fourni par l'évolution de la responsabilité dans le secteur des soins de santé de l'Ontario. La loi de 1991 sur les professions de la santé réglementées (*Regulated Health Professions Act, 1991*[102] (RHPA)), qui est entrée en vigueur le 31 décembre 1993, a établi un cadre commun de réglementation des fournisseurs des soins de santé dans les 23 professions réglementées de la santé en Ontario. Avec une série d'actes propres à la profession, cette loi réglemente à la fois les praticiens eux-mêmes ainsi que la pratique des diverses professions[103].

La base de toutes les lois de réglementation de la santé qui régissent les fournisseurs des soins de santé est celle de la protection du public (c'est-à-dire la protection des patients contre les praticiens de la santé qui sont incompétents, qui ne doivent pas exercer leur profession, etc.). La raison d'être de la protection du public se fonde sur la croyance que des praticiens réglementés offrent une meilleure qualité de soins de santé que ceux qui sont déréglementés. Toutefois, vers les années 1980, les gouvernements au Canada et aux États-Unis ont reconnu les lacunes de la réglementation dans divers autres secteurs de l'économie. Même si le gouvernement de l'Ontario a reconnu les coûts sociaux de la réglementation des fournisseurs des soins de santé et a compris qu'il n'était pas prudent ni possible de déréglementer les professions de la santé, la loi RHPA visait à diminuer les effets défavorables de la réglementation. Contrairement à la loi qui la précédait, la RHPA était conçue de manière à éviter trois aspects préjudiciables des règlements antérieurs :

1. Limitation excessive imposée à la liberté de choix du patient;
2. Entrave à l'évolution des rôles des diverses professions de la santé et
3. Limitations imposées à l'utilisation créative des professionnels de la santé.

Comme ce fut le cas dans le système de réglementation précédent, la RHPA a gardé le concept d'autoréglementation des professions de la santé. Toutefois, les organismes de réglementation

---

[100]James Casey & Frances Picherack, *The Regulation of Complementary and Alternative Health Care Practitioners: Policy Considerations*, Division des systèmes de santé – Santé Canada (décembre 2000), en ligne : <http://www.hc-sc.gc.ca/hppb/healthcare/pubs/comp_alt/regs.html#t3>.
[101]*Ibid.*
[102]S.O. 1991, c. 18.
[103]Linda S. Bohnen, *Regulated Health Professions Act- A Practical Guide* (Toronto: Canada Law Book, 1994) at 1.

(les ordres des professionnels de la santé ou Health Regulatory Colleges) devaient fonctionner avec une plus grande transparence et une plus grande responsabilité envers le public.

La Loi de 1991 sur les professions de la santé réglementées comprend de nombreuses règles sur la responsabilité. Les ordres des professionnels de la santé ainsi que leurs membres ont l'obligation légale de servir et de protéger l'intérêt du public et ils sont responsables envers les patients ainsi qu'envers le grand public. Quelques-unes des plus importantes dispositions de la loi qui portent sur la responsabilité comprennent les articles sur la structure des conseils des ordres, les responsabilités et les pouvoirs des conseils, les programmes sur les relations avec les patients, les registres des ordres, le processus des plaintes et des mesures disciplinaires, les dispositions sur la divulgation au public et la composition du Conseil consultatif[104].

En vertu de la Loi, les professionnels de la santé sont responsables à la fois envers leurs patients et envers le public. Les ordres des professionnels de la santé doivent servir l'intérêt public et ils ont l'obligation de rendre compte au public à ce sujet. L'efficacité de la Loi pour ce qui est de promouvoir et d'assurer la responsabilité entre les professionnels de la santé requiert que la RHPA établisse des dispositions suffisantes en matière de responsabilité. Il incombe aux ordres des professionnels de la santé de s'assurer que ces dispositions sont mises en œuvre de manière optimale[105].

Chaque ordre a un conseil qui fonctionne comme un conseil d'administration. Tous les conseils des ordres doivent avoir des membres du public qui ne sont pas des professionnels de la santé réglementés (même si les membres professionnels sont toujours en majorité). Pour assurer davantage la responsabilité envers le public, celui-ci a le droit d'assister aux réunions du conseil (sauf dans des circonstances rares et limitées).

La principale responsabilité du conseil d'un ordre est de gouverner la profession dans l'intérêt du public en s'assurant que ses membres se conforment à la Loi de 1991 sur les professions de la santé réglementées (RHPA) et qu'ils sont responsables auprès du public. La Loi assure et maintient cette responsabilité en demandant aux ordres de faire rapport annuellement au ministère de la Santé et des Soins de longue durée et en obligeant les conseils des membres à inclure des membres du public, comme il a été mentionné auparavant.

Les fonctions du conseil de l'ordre englobent l'établissement et la tenue à jour de normes sur les exigences en matière d'affiliation à l'ordre, sur l'assurance de la qualité, la portée de la pratique et l'éthique professionnelle. Les conseils ont également le pouvoir d'établir des règlements qui ont la même force de loi que la RHPA. En ce qui concerne l'obligation de rendre des comptes au public, quelques-uns des sujets les plus importants traités dans les règlements comprennent la définition de l'inconduite professionnelle et des conflits d'intérêt, les restrictions sur la publicité faite par des professionnels de la santé, les paramètres et les exigences de la tenue des dossiers et les règles concernant la délégation des actes contrôlés.

---

[104]Conseil consultatif de réglementation des professions de la santé de l'Ontario, *Weighing the Balance – A Review of the Regulated Health Professions Act – Request for Submissions*, (Toronto: Publications Ontario, 1999) à 20, en ligne : Health Professions Regulatory Advisory Council, <http://www.hprac.org/downloads//fyr/weighing.pdf>.
[105]*Ibid*. à 24.

Une autre fonction importante de la Loi lorsqu'il s'agit d'assurer et de maintenir la responsabilité envers le public, c'est que la Loi exige de chaque ordre qu'il établisse un programme de relations avec les patients afin d'aider à prévenir et/ou à traiter les cas de mauvais traitements d'ordre sexuel infligés à des patients, y compris le financement de la thérapie et des consultations. Ces programmes ont pour fonction d'éduquer les membres des ordres et d'informer le public de ce qu'est ou n'est pas une conduite professionnelle appropriée.

Chaque ordre des professionnels de la santé doit tenir à jour un registre qui contient de l'information au sujet des membres de l'ordre, y compris les mesures disciplinaires, l'information sur l'incompétence ou l'inconduite professionnelle, sur les modalités ou limitations indiquées dans le certificat d'inscription du membre, sur la suspension ou la révocation du certificat d'inscription du membre, etc. Étant donné que tout le monde, y compris les membres du public, peut obtenir cette information, la responsabilité envers le public est maintenue et renforcée.

La responsabilité envers le public est également une fonction importante de la procédure des plaintes et des mesures disciplinaires. Toutes les plaintes officielles sont examinées par un sous-comité du comité chargé de faire enquête sur les plaintes. Ce sous-comité doit avoir au moins un membre du public. Après l'examen de toutes les présentations et preuves, le comité chargé des plaintes peut renvoyer l'affaire au comité chargé de la discipline pour qu'il prenne éventuellement des mesures disciplinaires. Chaque ordre des professionnels de la santé doit inclure dans son rapport annuel un résumé des décisions du comité chargé de la discipline ainsi que les motifs de ces décisions. L'information au sujet des membres qui ont été trouvés coupables d'inconduite professionnelle par un comité de discipline est accessible au public.

Pour que la responsabilité globale soit maintenue, le Conseil consultatif de réglementation des professions de la santé (Conseil consultatif ou Advisory Council) a la responsabilité d'examiner l'impact et l'efficacité de la Loi de 1991 sur les professions de la santé réglementées (RHPA). Le Conseil consultatif est un organisme impartial qui n'est pas lié au ministère de la Santé et des Soins de longue durée. Les membres du public sont nommés par le gouvernement et ils ne doivent pas être des fonctionnaires, des employés de l'État, d'anciens membres ou des membres actuels du conseil d'un ordre ou d'un ordre professionnel.

7.2.2 Leçons en matière de responsabilité

Divers participants dans le secteur estiment que l'autoréglementation est appropriée et fonctionne bien lorsque les critères suivants sont remplis :

1. Il y a des normes de pratique de la profession ou des normes de l'industrie qui sont clairement définies et délimitées. Dans le cas des professions, la portée de la pratique doit être bien définie et délimitée.
2. Il doit y avoir un organisme bien constitué qui surveille, coordonne et facilite le processus d'autoréglementation. Dans le cas des professions de la santé au Canada, ces entités sont généralement connues sous le nom d'ordres professionnels.
3. Il doit y avoir des mécanismes intégrés au système d'autoréglementation afin d'assurer un niveau optimal de responsabilité et de transparence par rapport au public. Dans le cas des ordres des professionnels de la santé, cela signifie l'inclusion des membres du public

dans les conseils de l'ordre et le fait de s'assurer que les réunions du conseil sont accessibles au public (sauf dans des cas précis et limités lorsque des réunions ouvertes à tous ne sont pas faisables).

4. Les lois délégatrices (et les règlements) devraient clairement indiquer les pouvoirs et les devoirs des entités d'autoréglementation.

Il convient de noter qu'il y a une tension intrinsèque à permettre aux professions d'être autoréglementées. Même si on peut soutenir que les professionnels sont le mieux en mesure d'évaluer les normes et les pratiques de leurs pairs, on peut avancer l'argument contraire selon lequel ceux qui agissent pour réglementer l'entrée dans une profession ou la pratique de cette profession ne peuvent pas le faire équitablement s'ils doivent profiter de leurs propres mesures de réglementation (par exemple, en réduisant la concurrence sur le marché grâce à l'établissement, sans raisons valables, de normes élevées d'entrée dans la profession).

7.3 Le secteur des services financiers

7.3.1 Évolution du concept de responsabilité

Au Canada, avant la Confédération (et comme dans de nombreux autres pays), l'activité bancaire s'est développée afin de satisfaire aux besoins des échanges et du commerce. L'une des premières théories sur la fonction des banques dans l'économie cherchait à expliquer comment les changements de la masse monétaire devraient être liés aux besoins du commerce. Cette théorie, connue sous le nom de doctrine des « Real Bills », déclarait que la croissance de la masse monétaire devrait être liée à la croissance de la production au moyen du crédit à court terme (ce qui signifiait alors des billets de banque privés). Par ce mécanisme, la masse monétaire serait toujours garantie par la production de l'économie, assurant ainsi un niveau stable des prix[106].

Le développement initial du secteur financier au Canada a été influencé par un point de vue fondé sur la responsabilité selon lequel le bien-être de la société dans son ensemble stipule que l'industrie bancaire doit être réglementée dans une certaine mesure. Ainsi, les premiers développements et l'évolution du secteur financier au Canada ont été influencés par ce point de vue ainsi que par l'approche conservatrice adoptée en Angleterre dans le domaine bancaire. Toutefois, ce conservatisme a été tempéré par les expériences de systèmes bancaires libres[107] qui ont été menées aux États-Unis et en Écosse de 1800 à 1850. Selon le paradigme de système bancaire libre, les particuliers et les entreprises chercheront à conclure des ententes avec les établissements afin de minimiser les coûts de la conduite des affaires. La concurrence entre les banques est censée stimuler la stabilité du système, éliminant ainsi la nécessité d'avoir recours à une banque centrale (prêteur de dernier recours).

[106]Pierre L. Siklos, *Money, Banking and Financial Institutions – Canada in the Global Environment*, 2d ed. (Toronto: McGraw Hill Ryerson Limited, 1997) à 390.

[107]Le système bancaire libre (« Free Banking ») est un système financier qui est fortement déréglementé et où il y a peu de barrières gouvernementales à l'entrée.

La perspective contraire sur l'évolution d'un système bancaire est couramment connue sous le nom de point de vue des restrictions légales (« Legal Restrictions View »). Ce paradigme énonce que seule la réglementation forcera le public à détenir des obligations (la dette) du gouvernement qui ne produisent pas d'intérêts (c'est-à-dire la monnaie). La stabilité du système financier ne sera assurée que s'il y a un certain niveau de réglementation et de contrôle de la part du gouvernement.

Au cours du 18e siècle et au début du 19e siècle, l'une des fonctions des établissements bancaires (qui est aussi importante que le fait d'accepter des dépôts et d'accorder des prêts) était celle de l'émission des billets de banque. Comme la Grande-Bretagne avait établi la tradition d'un système bancaire conservateur et prudent, les chartes de banques étaient assez difficiles à obtenir dans les colonies britanniques comme le Canada. Après l'échec de plusieurs entreprises bancaires qui appartenaient à des groupes de commerçants montréalais vers la fin du 18e et au début du 19e siècle, la Banque de Montréal a obtenu une charte pour fonctionner comme banque en 1822. La Banque du Nouveau-Brunswick et la Banque du Haut-Canada ont obtenu leur charte en 1820 et 1821, respectivement. Ces premières chartes de banque autorisaient l'établissement bancaire à émettre des billets, à faire des prêts à des fins commerciales jusqu'à un montant stipulé et à ouvrir généralement des succursales. Un trait commun à toutes ces chartes était que l'institution financière devait rendre compte au gouvernement en faisant des rapports sur l'état de ses activités financières à intervalles réguliers[108].

Par conséquent, le paradigme du système bancaire conservateur fondé sur le modèle britannique, caractérisé par la réglementation et la responsabilité à l'égard du gouvernement, est devenu le modèle de l'évolution et du développement des banques au Canada.

En réponse aux objections des populistes selon lesquelles les chartes des banques étaient essentiellement accordées aux personnes qui avaient les « bons » liens sociopolitiques, surtout dans les régions urbaines, la législature du Haut-Canada a déposé une loi en 1850 sur un système bancaire libre qui était fondé sur les lois bancaires de l'État de New York à cette période. Toutefois, il y avait un certain niveau de responsabilité sous forme de réglementation limitée. Par exemple, des règlements spécifiaient le minimum du capital de démarrage requis, outre le fait que les billets de banque devaient être remboursables en argent sur demande.

À la Confédération, la *Loi constitutionnelle de 1867* accordait le monopole de toutes les questions bancaires et d'émission de la monnaie au tout nouveau gouvernement fédéral du Canada. La première *Loi sur les banques* a été promulguée par le Parlement en 1871 et ce sera la première d'une série de lois qui réglementent les activités de toutes les banques à charte du Canada. Ses points saillants incluaient la définition d'une banque à charte, l'introduction graduelle d'un monopole gouvernemental dans l'émission de la monnaie et une stipulation selon laquelle la législation devait être révisée tous les dix ans.

Les thèmes prédominants dans la série des *Lois sur les banques* portaient sur la sécurité bancaire et sur l'élargissement de la portée des opérations des banques à charte. La question de la sécurité bancaire a été traitée explicitement pour la première fois en 1891 lorsque le Fonds de

[108] *Ibid*. à 392.

remboursement des billets de banque en circulation (Bank Circulation Redemption Fund) a été établi comme mesure de protection contre la perte des fonds en cas de faillite des banques. La preuve que la responsabilité financière ne cesse de croître est apparente dans l'exigence toujours croissante en matière de vérification des activités bancaires, exigence qui a culminé dans l'établissement d'une surveillance gouvernementale du système bancaire. En outre, la responsabilité à l'égard du public a encore augmenté en 1967 avec l'établissement de la Société d'assurance-dépôts du Canada (SADC/CDIC).

Un développement important dans l'évolution de la responsabilité dans le secteur financier a été celui de l'établissement de la Banque du Canada en 1935. La diminution de la masse monétaire pendant et après la Grande dépression a été considérée comme un échec de l'entente préétablie sur la politique monétaire. En outre, l'étalon-or n'a plus eu cours dans les années 1930. Les forces politiques ont également contribué à la nécessité d'avoir une banque centrale, y compris à la nécessité pour le Canada de coordonner ses politiques économiques internationales avec celles du reste du monde.

La Banque du Canada a pour mandat d'assurer la politique monétaire du Canada et de faciliter la croissance de l'activité économique tout en maintenant de faibles taux de chômage. La banque fonctionne de manière à créer une plus grande responsabilité dans le système financier en contrôlant la politique monétaire grâce au rajustement des taux d'intérêts et à la gestion de la base monétaire. En outre, elle mène des opérations sur le marché libre, elle agit comme agent fiscal du gouvernement fédéral et elle fonctionne comme le prêteur de dernier recours.

La « période dite moderne » (à partir des années 1970 jusqu'à présent) a été caractérisée par une législation financière qui visait à libéraliser les règlements régissant le comportement des banques à charte. Tout comme la plupart des gouvernements d'autres pays, le Canada a instauré la déréglementation dans plusieurs aspects du secteur bancaire. Cela a permis aux banques à charte d'offrir une vaste gamme de produits et services, y compris les services des prêts hypothécaires à l'habitation, le crédit-bail financier et les services de traitement des données. À partir des années 1980, les banques à charte ont eu le droit d'acquérir des firmes de courtage.

La *Loi sur les banques* de 1991 a donné lieu à un environnement de réglementation qui a stimulé une concurrence quasi égale dans tout le secteur financier au Canada. Cela a pratiquement éliminé l'approche historique des « quatre piliers » qui avait été adoptée pour les établissements financiers canadiens et qui comprenait les banques à charte (prêts commerciaux), les sociétés de fiducie et les caisses populaires (prêts personnels), les compagnies d'assurance et les courtiers en valeurs mobilières. Cette Loi a essentiellement établi un ensemble complet de réformes pour tous les types d'institutions financières au lieu de l'ancien système où l'on légiférait pour une branche du secteur financier séparément des autres.

Les banques au Canada ont joui d'énormes avantages, y compris la croissance extraordinaire des actifs, des profits annuels records et la domination du marché à la suite de décennies de protections et de privilèges qui leur étaient offerts par le gouvernement canadien. L'actif de

chacune des cinq grandes banques dépasse les revenus annuels du gouvernement fédéral[109]. Même si de nombreux critiques ont soutenu que les banques ne seraient pas aussi grandes ni aussi profitables si elles n'avaient pas ces protections et privilèges et bien que de nombreux Canadiens soient insatisfaits de certains aspects des pratiques et politiques des banques, peu d'entre eux nieront que les banques ont une grande confiance du public quant à l'argent qu'elles gèrent. En outre, les consommateurs doivent être protégés par rapport au secteur financier.

C'est pour ces raisons qu'il y a un besoin continu de règlements/de lois pour assurer la responsabilité appropriée dans le secteur financier.

Le gouvernement fédéral reconnaît la nécessité de réglementer le secteur des services financiers. Comme l'indique le document de travail sur l'examen de la législation dans le secteur financier de 1997 :

> « Il ne fait aucun doute que le besoin de réglementation se fait sentir dans le secteur financier. Non seulement des réglementations protégeraient-elles le consommateur, mais elles permettraient de définir les règles du jeu afin que le secteur puisse déployer ses activités harmonieusement[110]. »

En outre, les divers groupes de participants qui représentent les consommateurs, les petites entreprises et les intérêts communautaires ont demandé instamment au gouvernement fédéral de modifier/d'étendre la législation et les règlements actuels de manière à assurer une plus grande responsabilité et une meilleure équité.

7.3.2 Vérification financière

Comme on peut le voir dans la section précédente, le secteur des services financiers représente un segment vital de l'économie nationale. La principale raison en est que ce secteur est intimement associé à la fois à la politique fiscale et à la politique monétaire. Ce secteur contrôle fortement la création et les flux monétaires au moyen de l'économie.

Des mesures fiables et précises dans le secteur des services financiers ont une importance extrême à cause de la nécessité de quantifier les flux monétaires. Étant donné que la comptabilité des flux monétaires est si cruciale, on a établi et mis en œuvre des normes appelées Principes comptables généralement reconnus (PCGR/GAAP). L'explication et la définition complètes des PCGR (provenant du Collège du commerce à l'Université de Saskatchewan) sont reproduites ci-dessous :

> L'expression « Principes comptables généralement reconnus » dans le rapport du vérificateur comprend non seulement la notion étroite de principes spécifiques associés à la comptabilité (par exemple, principe du coût historique, principe du rapprochement, principe de matérialisation des revenus), mais aussi les politiques spécifiques (méthodes),

---

[109]Coalition canadienne pour le réinvestissement communautaire, « Un système d'imputabilité pour les institutions financières du Canada : Comment s'assurer qu'elles satisfont à des normes élevées (An Accountability System For Financial Institutions in Canada: How To Ensure They Meet a High Standard of Performance) », *cinquième exposé de position de la CCRC* (décembre 1997), en ligne : site Web de la CCRC <http://www.cancrc.org/english/pp5sum.html>.

[110]*Ibid.*

> les pratiques, les procédures et les règles qui servent à déterminer ce qui est inclus dans les états financiers, comment les montants sont déterminés (les mesures prises), comment les articles sont classifiés et quelles divulgations sont faites (par exemple, les notes). Bien entendu, les Principes comptables généralement reconnus incorporent toutes les exigences des recommandations du Manuel de l'Institut canadien des comptables agréés (ICCA). Au-delà de ce point, les « principes » appliqués reflètent ce qui est fait par un nombre important de sociétés canadiennes pour des articles semblables ou ce qui est appuyé dans des ouvrages canadiens autres que le Manuel de l'ICCA ou encore dans les normes du Conseil des normes comptables internationales (IASC) ou de pays étrangers (particulièrement les États-Unis). Lorsqu'on s'éloigne du Manuel de l'ICCA ou que l'on interprète son contenu en cas de solutions de rechange acceptables ou d'une recommandation quelque peu générale, il faut se servir de son jugement professionnel pour établir qu'un « principe » utilisé est justifiable et approprié à la situation.
>
> La théorie comptable (cadre de travail conceptuel sur les objectifs, les concepts pertinents, etc.) devrait être déduite des PCGR cités dans les rapports de vérification. La définition des principes comptables généralement reconnus (PCGR) du Manuel de l'ICCA incorpore la vaste base conceptuelle de la comptabilité financière. Avant que la définition soit mise dans le Manuel (mars 1991), bien des personnes ne pensaient pas que la théorie faisait partie des PCGR, mais elles la considéraient toujours comme une base générale d'établissement des PCGR. Toutefois, cette théorie a probablement joué un rôle important de façon implicite dans l'exercice du jugement professionnel.
>
> Les principes comptables généralement reconnus sont les principes (que leur utilisation soit limitée ou non) qui sont particulièrement bien fondés. Reconnaître ou non qu'un principe donné est digne de foi est une question de fait et de jugement. Le comptable et le vérificateur sont tous deux responsables de la collecte des preuves évidentes du bien-fondé des principes et ils doivent juger si c'est suffisant pour les mettre en pratique dans les limites des principes comptables généralement reconnus.
>
> La source de base des principes comptables généralement reconnus au Canada est le Manuel de l'ICCA. La *Loi canadienne sur les sociétés par actions* établit ce manuel comme le document de base qui détermine les lois du pays en ce qui concerne les normes comptables financières et les divulgations dans le cas des compagnies constituées en vertu de la loi. Même s'il a une importance primordiale, le Manuel de l'ICCA laisse fréquemment beaucoup de place au jugement sur la signification des normes, et par conséquent, sur l'importance d'autres sources qui font autorité[111].

Afin de s'assurer que les principes comptables généralement reconnus sont bien appliqués, un mécanisme de contrôle tiers a été établi et on l'appelle la vérification financière. Les vérificateurs qui conduisent et mettent en œuvre la vérification ne contrôlent pas eux-mêmes les mesures financières déclarées. Par conséquent, l'établissement des services financiers a compris qu'on ne pouvait pas tenir les vérificateurs responsables de l'exactitude des états financiers. *Bien plutôt, le vérificateur est responsable du processus et non pas des résultats de la vérification* puisqu'il n'a aucun contrôle sur le comportement de la société dont les états financiers sont vérifiés.

---

[111]College of Commerce-University of Saskatchewan, Commerce 321 Course, « Solution to Assignment #1 » (2002), en ligne : College of Commerce-University of Saskatchewan <http://www.google.ca/search?q=cache:OzP6wSXzfgYJ:www.commerce.usask.ca/faculty/kobussen/Comm_321/Solution_to_Assignment_1.doc+%22definition+of+GAAP%22&hl=en&ie=UTF-8>.

7.3.3 Leçons en matière de responsabilité

Divers participants dans le secteur ont offert les opinions suivantes concernant les leçons en matière de responsabilité :

- Lorsqu'on détermine que la fourniture d'un produit ou d'un service essentiel est réalisée de la meilleure façon possible par un oligopole restreint, la réglementation du secteur public est souvent appropriée. Cela s'applique également à une situation de monopole.
- Dans les cas où l'environnement d'exploitation canadien est à la fois instable et connecté mondialement, il serait utile d'avoir un processus formel d'examen et de mise à jour des règlements et des lois sur une base permanente. C'est nécessaire afin de s'assurer que ces lois et règlements restent pertinents et efficaces.
- Si nous voulons tenir les personnes et les entités responsables de leurs actions, il est essentiel d'avoir des outils de mesure fiables et sûrs pour faciliter le processus, par exemple, des normes, des bancs d'essais et/ou des procédures spécifiques (les PCGR en sont un bon exemple).
- Si une entité n'exerce pas un contrôle total sur tous les aspects d'une situation, le mieux que l'on puisse faire, c'est que l'entité soit tenue responsable de son processus, mais non de ses véritables résultats (comme c'est le cas pour les vérificateurs financiers).

7.4 Services d'électricité

7.4.1 Évolution du concept de responsabilité – L'expérience américaine

Contrairement à l'infrastructure d'information essentielle, le secteur de l'alimentation électrique représente une industrie évoluée et établie. La California Electric Company de San Francisco, fondée en 1879, a été la première compagnie qui a été lancée dans le but de vendre de l'électricité. L'énergie électrique était vendue à des entreprises commerciales et à des usines pour alimenter les lampes à arc électriques[112]. Cela a été suivi trois ans plus tard par l'ouverture de la centrale d'énergie électrique Thomas Edison à Pearl Street dans le bas Manhattan; cette centrale fournissait du courant continu (c.c.) pour l'éclairage incandescent d'une zone d'environ un sixième de mille carré. Au cours des 20 années suivantes, de petites centrales électriques étaient bâties dans des villes de toutes tailles. Au début du 20^{e} siècle, plus de 3 000 centrales électriques étaient exploitées aux États-Unis.

En 1881, Lucien Gaulard et John D. Gibbs ont breveté en Angleterre le premier système de transmission de courant alternatif (c.a.). Les brevets américains du système ont été acquis en 1885 par George Westinghouse et la première transmission commerciale de courant alternatif aux États-Unis a eu lieu en 1890 sur une ligne de 3 300 volts, de Willamette Falls à Portland, en Oregon.

Dans les premières années de l'industrie électrique, la responsabilité était pratiquement inexistante. Les centrales électriques et les installations de distribution étaient alors la propriété

[112]Luces M. Faulkenberry & Walter Coffer, *Electrical Power Distribution and Transmission*, (Englewood Cliffs: Prentice-Hall, Inc., 1996) à 7.

de particuliers ou de petits groupes d'investisseurs. Dans certains cas, les personnes produisaient de l'électricité pour leur propre usage domestique et vendaient l'excédent à leurs voisins. D'autres établissaient de petites centrales et vendaient l'électricité à tous ceux qui voulaient l'acheter. Certaines centrales électriques étaient ouvertes et exploitées par des entrepreneurs à la recherche d'une entreprise profitable[113].

Étant donné que chaque génératrice devait être reliée au client qu'elle servait, de nombreuses localités avaient des systèmes de distribution d'électricité en double. Cette situation a donné lieu à trois problèmes principaux :

1. Les nombreuses lignes de transmission peu espacées et qui se croisaient ont créé un danger potentiel pour la vie et la propriété;
2. Il y avait une accumulation inacceptable de droits de passage publics résultant des nombreux systèmes de distribution et
3. Les nombreux systèmes de distribution en double entraînaient des coûts en capital extrêmement élevés, ce qui provoquait alors des tarifs élevés d'électricité.

La première tentative d'établissement de la responsabilité a été faite lorsque des franchises ont été octroyées à un seul fournisseur d'énergie électrique pour une seule zone géographique. En 1900, quelques-unes des petites compagnies d'électricité qui étaient en concurrence se sont regroupées en entreprises franchisées plus importantes qui sont devenues la propriété des investisseurs.

Même si cette étape a résolu les trois problèmes mentionnés, elle a créé un nouveau problème, soit la nécessité d'avoir le moyen de contrôler les tarifs d'électricité puisque les forces concurrentielles ne pouvaient plus les gouverner. Ce problème a été résolu grâce à la réglementation. L'État de New York a établi la première commission de réglementation des services publics en 1905, ce qui a marqué le début du passage du secteur de production et de distribution de l'électricité à des monopoles réglementés par l'État. En 1924, 42 États avaient créé des commissions de réglementation des services publics d'électricité. La Federal Power Commission a été établie en 1920 pour accorder les permis de construction et d'exploitation de centrales hydroélectriques.

Au début du développement de l'industrie de l'électricité (de 1914 à 1916), on a établi les raisons pour lesquelles les services publics d'électricité devaient être des monopoles réglementés. Ces raisons sont encore jugées valides aujourd'hui. Tout d'abord, l'investissement en capital requis pour chaque unité de revenu reçue est bien plus élevé dans l'industrie de production et de distribution de l'électricité qu'il ne l'est dans d'autres secteurs. En second lieu, le fait d'avoir un service public d'électricité en double dans une zone géographique est coûteux et inefficace et c'est un gaspillage des ressources naturelles et des ressources humaines. Toutefois, afin d'assurer la responsabilité à l'égard du public, les monopoles doivent être réglementés, puisque ces services publics n'ont aucune concurrence. Les entités de réglementation elles-mêmes doivent être responsables envers le public pour garantir que des structures tarifaires et des pratiques commerciales appropriées sont suivies par les services publics. En outre, les services publics d'électricité doivent avoir un rendement adéquat de

[113] *Ibid*. à 7.

l'investissement de manière à assurer les améliorations nécessaires en capital et à attirer les investisseurs.

Un autre aspect de la responsabilité dans le secteur public de l'électricité est celui de la sécurité publique. Les compagnies de services publics ont la responsabilité de prendre des précautions raisonnables pour assurer la sécurité à la fois du public et de leurs propres employés. Les services publics doivent s'assurer qu'il n'y a pas d'actes préjudiciables pour les personnes ou les biens à cause d'un équipement inadéquat ou défectueux. Cet aspect de la sécurité est particulièrement vital dans le cas de la plus grande menace possible à la sécurité publique dans toute infrastructure essentielle, soit la menace des centrales nucléaires.

7.4.2 Évolution du concept de responsabilité – L'expérience canadienne

Dans la plupart des pays en dehors des États-Unis, le gouvernement est l'entité qui produit et qui distribue le courant électrique. Le système de transmission et de distribution de l'électricité au Canada est structuré de façon assez particulière puisqu'il reflète les idiosyncrasies historiques des compétences fédérales/provinciales et de la concurrence entre les provinces. Plutôt que d'établir un réseau national ou même des réseaux régionaux importants pour tirer parti des rendements et des possibilités de production à faible coût de quelques provinces, les querelles entre les provinces ont empêché l'établissement d'un mécanisme qui aurait pu réglementer la transmission de l'électricité au-delà des frontières provinciales. Au lieu de cela, chaque province a développé un réseau électrique de transmission et de distribution dans ses propres frontières. Plutôt que d'exporter de l'électricité vers d'autres provinces, une province exporterait de l'électricité vers les États-Unis à cause de sa morphologie de réseau unique. À la suite de cette évolution historique, les liens nord-sud sont beaucoup plus prédominants et plus développés que les liens entre les provinces[114].

Quant à l'évolution du concept de responsabilité, la plus grande partie de la réglementation est sous contrôle provincial puisque l'industrie de l'électricité s'est développée essentiellement dans les limites provinciales. Jusqu'à tout récemment, tous les gouvernements provinciaux étaient directement propriétaires des principaux services publics d'électricité ou assuraient un puissant contrôle de réglementation sur les monopoles privés. Cela a eu pour effet, dans la plupart des cas, de garder solidement dans le domaine public la sécurité de l'approvisionnement et la stabilité des prix. Le gouvernement fédéral réglementait l'exportation de l'électricité vers les États-Unis et il fallait obtenir l'approbation de l'Office national de l'énergie (ONE/NEB) avant de conclure tout accord d'exportation[115].

Ces accords étaient soumis à l'examen du public et à l'obligation de rendre des comptes au cours d'audiences afin d'en déterminer l'effet sur les divers groupes de participants et sur l'environnement. Toutefois, ce contrôle fédéral et l'examen du public ont commencé à changer avec l'ouverture graduelle du marché pour se conformer aux demandes de la FERC (Federal Energy Regulatory Commission) des États-Unis et avec la signature de l'Accord de

[114]Marjorie G. Cohen, « From public good to private exploitation: GATS and the restructuring of Canadian electrical utilities » *Canadian-American Public Policy* 48 (1er décembre 2001) 1, à 30.
[115]*Ibid*. à 33.

libre-échange entre le Canada et les États-Unis qui est devenu plus tard l'Accord de libre-échange nord-américain (ALENA).

Les services publics canadiens d'électricité ont compris que, s'ils voulaient augmenter les exportations vers les États-Unis, ils devaient commencer le processus de déréglementation de leurs marchés. La responsabilité globale en matière d'exportation de l'électricité a diminué à la suite des modifications apportées à la loi, modifications qui ont changé les fonctions de surveillance de l'Office national de l'énergie du Canada. Ces changements ont éliminé la nécessité de consulter le public au sujet de l'importance économique et sociale des exportations proposées. Les permis d'exploitation peuvent maintenant être accordés plus couramment sans audiences publiques et, dans la plupart des cas, sans examen du gouvernement fédéral. En réponse aux changements du marché, à la hausse des échanges en matière d'électricité et à l'augmentation des actions des services publics canadiens sur les marchés au comptant, des permis d'exportation généraux sont délivrés aux compagnies d'exportation. Par conséquent, la responsabilité est réduite puisqu'il n'y a pratiquement aucun contrôle ni surveillance sur les exportations canadiennes d'électricité[116].

En Ontario avant 1998, Hydro-Ontario, monopole intégré verticalement et propriété du gouvernement, avait la responsabilité de répondre aux besoins de la province en matière de production et de transmission de l'électricité. L'électricité produite par Hydro-Ontario était achetée et distribuée aux consommateurs par environ 300 compagnies locales d'électricité qui appartenaient aux municipalités et qui payaient un prix fixe par kilowatt-heure (kWh). Le prix global comprenait les coûts de production, de transmission et de distribution[117].

Hydro-Ontario avait accumulé une énorme dette au fil des années, ce qui doublé les prix de l'électricité vers la fin des années 1980 et au début des années 1990. Cette situation a été souvent attribuée aux méthodes de planification centralisées de l'organisation et au manque de « sérieuse responsabilité »[118]. Les critiques ont très souvent cité le manque de responsabilité d'Hydro-Ontario auprès de la législature de l'Ontario ou de toute autre entité. Le ministère de l'Énergie, des Sciences et de la Technologie a publié un livre blanc en 1997 où l'on signalait « une relation ambiguë » entre Hydro-Ontario et le gouvernement de l'Ontario.

Le gouvernement de l'Ontario a démantelé l'organisation Hydro-Ontario en 1998. À ce moment-là, les services municipaux d'électricité distribuaient également l'électricité acheminée par Hydro-Ontario. Ces services municipaux étaient réglementés par Hydro-Ontario. Le but du gouvernement était de déréglementer le secteur de l'électricité et de créer de la concurrence dans l'industrie. À la suite de ce démantèlement, cinq entités distinctes ont été créées à partir de l'ancienne organisation Hydro-Ontario. L'entreprise OPG (Ontario Power Generation Inc.) est devenue responsable de la production d'électricité et de la vente en gros de l'énergie électrique. Hydro One Inc. a assumé la transmission, la distribution rurale et la vente de détail des services

[116] *Ibid.*
[117] Michael J Trebilcock & Roy Hrab, « What will keep the lights on in Ontario: responses to a policy short-circuit? » *C.D. Howe Institute Commentary* 191 (1er décembre 2003) 1, à 3.
[118] David McFadden « Power to the people: The Opening of Ontario's electricity market is not just a get-rich scheme for a greedy few. It swill benefit the economy, the environment and consumers. » *The Financial Post (National Post)* (2 mai 2002) FP 15.

d'électricité. On a créé un exploitant indépendant du marché de l'électricité (IMO) pour qu'il soit le responsable sur le marché de la distribution de l'électricité et du contrôle du réseau de transmission. L'Office de la sécurité des installations électriques a été établi pour la conduite des inspections de l'équipement électrique et des installations de câblage. La Société financière de l'industrie de l'électricité de l'Ontario (SFIEO/OEFC) a assumé la responsabilité de la gestion de la dette en souffrance de l'ancienne organisation Hydro-Ontario[119].

La restructuration d'Hydro-Ontario n'a pas donné les résultats voulus, c'est-à-dire réduire la dette de la province dans le secteur de l'électricité, diminuer les prix de l'électricité et encourager l'investissement du secteur privé dans les installations de production de l'électricité. Bien plutôt, cette restructuration a entraîné des prix plus élevés et une nouvelle dette du secteur de l'électricité tout en décourageant l'investissement du secteur privé dans la production. La solution des problèmes d'électricité de l'Ontario peut être liée à une facette différente de la responsabilité (c'est-à-dire à une forme économique de responsabilité). Les producteurs et les consommateurs d'électricité doivent tous deux être soumis à des prix réalistes qui reflètent les conditions réelles de l'offre et de la demande. Il faut ce type de régime pour établir la viabilité financière et la stabilité à long terme du système d'électricité de l'Ontario. En outre, en exposant les consommateurs à des prix qui reflètent les conditions réelles du marché, on encouragera la demande en matière de conservation d'énergie et d'utilisation de produits efficaces sur le plan énergétique. Dans la même veine, le fait de lier les prix aux conditions du marché produirait des pressions du côté de l'offre, ce qui stimulerait l'investissement dans un équipement et dans des installations efficaces de production et de transmission[120].

En ce qui concerne les centrales nucléaires, un degré élevé de responsabilité a été imposé par la législation. L'article 3 de la *Loi sur la responsabilité nucléaire*[121] signale en partie :

> Obligation imposée à un exploitant
>
> « 3. Sous réserve des autres dispositions de la présente loi, un exploitant a l'obligation de voir à ce qu'aucune blessure à une autre personne ou qu'aucun dommage aux biens d'une autre personne ne soient occasionnés à la suite des propriétés fissiles ou radioactives ou d'une combinaison de l'une de ces propriétés avec des propriétés toxiques, explosives ou autres propriétés dangereuses d'une substance nucléaire qui, selon le cas a) est dans l'installation nucléaire dont il est l'exploitant. »

L'article 4 impose la responsabilité maximale lorsqu'il déclare :

> Responsabilité absolue de l'exploitant
>
> « 4. Sous réserve des autres dispositions de la présente loi, un exploitant est, sans preuve de faute ou de négligence, responsable absolument d'une violation de l'obligation que lui impose la présente loi. »

[119]Cohen, *supra* note 114 à 55 - 56.
[120]Trebilcock & Hrab, *supra* note 117 à 19.
[121]*Loi sur la responsabilité nucléaire (Nuclear Liability Act)*, R.S., c. 29 (1st Supp.), ss. 3 – 4.

La *Loi sur la responsabilité nucléaire* a un double objet :

1. Assurer la disponibilité des fonds nécessaires pour accorder une compensation financière à des tiers en dédommagement des blessures ou dommages subis par suite d'un accident nucléaire, en obligeant l'exploitant à assumer l'absolue responsabilité, sans égard à la faute et
2. Établir un régime de responsabilité nucléaire qui encourage la production d'énergie nucléaire en attribuant toute responsabilité civile à l'exploitant, tout en limitant la responsabilité de celui-ci[122].

Le régime de responsabilité établi dans la *Loi sur la responsabilité nucléaire* est semblable à celui que l'on trouve dans la législation intérieure de la plupart des pays qui utilisent l'énergie nucléaire ainsi que dans les deux principales conventions internationales sur la responsabilité de tiers, soit la Convention de Paris et la Convention de Vienne. La Convention de Paris (essentiellement une convention de l'Europe de l'Ouest) a été adoptée sous les auspices de l'Organisation de coopération et de développement économiques (OCDE) en 1960. La Convention de Vienne, qui a un plus grand nombre de membres, est une convention de l'Agence internationale de l'énergie atomique (AIEA) qui a été adoptée en mai 1963.

La *Loi sur la sûreté et la réglementation nucléaires*[123] (LSRN) a reçu la sanction royale le 20 mars 1997 et elle est entrée en vigueur le 31 mai 2000. La LSRN a remplacé la *Loi sur le contrôle de l'énergie atomique* de 1946 par une nouvelle législation plus efficace et plus explicite afin de réglementer les activités de l'industrie nucléaire canadienne. La LSRN a également permis l'établissement de la Commission canadienne de sûreté nucléaire (CCSN) qui a remplacé la Commission de contrôle de l'énergie atomique (CCEA).

7.4.3 Leçons en matière de responsabilité

Divers participants dans le secteur ont offert les opinions suivantes concernant les leçons en matière de responsabilité :

- Les producteurs ainsi que les consommateurs des produits ou services d'un monopole réglementé doivent être tenus responsables des conditions économiques et des forces du marché qui reflètent les véritables conditions de l'offre et de la demande dans le secteur. C'est important si on veut que l'industrie reste financièrement stable et économiquement viable.
- Un tel régime de « responsabilité économique » aidera également à promouvoir l'utilisation efficace des produits ou services et à attirer de nouveaux capitaux et investissements pour bâtir une capacité d'exécution ou de production efficace.

[122]Direction des ressources en électricité de Ressources naturelles Canada, *page Web sur l'énergie nucléaire (Nuclear Legislation Web Page),* (6 mars 2003), en ligne : Natural Resources Canada – Nuclear Energy, <http://www2.nrcan.gc.ca/es/erb/erb/english/View.asp?x=453>.
[123]*Loi sur la sûreté et la réglementation nucléaires (Nuclear Safety and Control Act)* (1997, c. 9).

7.5 Services juridiques

7.5.1 Introduction

La pratique du droit au Canada, comme dans la plupart des pays du Commonwealth, est une profession autoréglementée. En l'absence d'une intervention gouvernementale, des avocats (à quelques exceptions près) sont élus par d'autres avocats pour surveiller l'admission, la compétence, la réglementation et le processus disciplinaire des avocats dans chacune des provinces. Aux États-Unis, au contraire, la profession juridique est gouvernée par la réglementation judiciaire. Chaque province a son propre barreau qui est chargé de réglementer la communauté juridique dans la province. Nous examinerons l'organisme directeur de l'Ontario, soit le Barreau du Haut-Canada, car c'est un organisme représentatif des barreaux.

Afin d'exercer le droit en Ontario, un avocat doit être membre du Barreau. Le Barreau du Haut-Canada a pour mission

> de réglementer la profession juridique dans l'intérêt public :
>
> - En veillant à ce que les avocates et les avocats, qui sont au service de la population de l'Ontario, répondent à des normes élevées en matière de formation, de compétence et de déontologie;
> - En défendant l'indépendance, l'intégrité et l'honneur de la profession juridique;
> - Aux fins de la promotion de la justice et de la primauté du droit[124].

Quarante avocats élus et huit non-juristes nommés constituent le corps dirigeant du Barreau et on les appelle des conseillers. Les conseillers se réunissent une fois par mois (à la Convocation) pour traiter des questions de gouvernance et pour prendre les décisions de principe. Les conseillers forment également des comités pour instruire les affaires de conduite et de compétence des avocats.

7.5.2 Historique

Jusqu'en 1792, un avocat de l'Ontario était ce que les gouverneurs britanniques de la ville de Québec décrétaient être un avocat. Les tribunaux avaient le pouvoir d'inscrire les avocats au barreau et d'établir des normes. Il n'y avait aucune exigence officielle de formation des avocats en Ontario jusqu'en 1785. Avec l'adoption de *Judicature Act* en 1794, les tribunaux coloniaux ont été remplacés par les procédures et les structures plus institutionnalisées du système britannique. Comme on manquait d'avocats formés dans le Haut-Canada (maintenant l'Ontario) à ce moment-là, une loi a été adoptée autorisant le Lieutenant Gouverneur à accorder à 16 personnes le permis d'exercer en tant qu'avocats pendant deux ans. Après la période de deux ans, le droit d'inscrire des avocats au barreau revenait aux tribunaux.
En juillet 1797, une loi intitulée *An Act for the Better Regulating the Practice of Law* (Loi visant une meilleure réglementation de l'exercice du droit) a été adoptée. La Loi donnait naissance au Barreau :

> …il peut et doit être légitime pour les personnes maintenant admises à pratiquer le droit et à exercer au barreau dans l'un des tribunaux de Sa Majesté dans cette province de se

[124]Mission du Haut-Canada (Role Statement of the Law Society of Upper Canada), adoptée à la Convocation le 27 octobre 1994.

> constituer en société sous le nom de Law Society of Upper Canada et d'établir l'ordre entre elles afin de doter la province d'un corps savant et honorable…

La Loi a donné au Barreau nouvellement formé le droit d'établir des règles et des règlements pour régir la profession juridique dans le Haut-Canada. Cette capacité de se gouverner et de se réglementer ne provient pas des systèmes britanniques ou américains qui régissent la profession d'avocat. Ces deux juridictions étaient réglementées par les tribunaux. Les raisons qui sous-tendent la décision de créer le Barreau et de lui permettre de régir la profession semblent être perdues puisque les dossiers du gouvernement de ce temps-là ont brûlé pendant l'occupation américaine de York (maintenant Toronto) en 1813.

Contrairement aux États-Unis et à d'autres provinces canadiennes qui ont accordé aux universités le droit de former les avocats, le Barreau a contrôlé l'enseignement du droit. En 1949, le doyen, avec la plupart des membres de la faculté de droit du Barreau, a fait défection et est allé à l'Université de Toronto pour constituer l'école de droit de l'université. En 1957, le Barreau et les universités provinciales ont convenu que n'importe quelle université dans la province pouvait ouvrir une école de droit. Pour y être admis, il fallait avoir suivi un programme de deux ans de premier cycle. Après trois années d'études universitaires en droit, les étudiants devaient faire un stage d'un an suivi de six mois de formation professionnelle au Barreau. Ce mode de formation des étudiants pour devenir des avocats en Ontario reste plus ou moins inchangé à ce jour.

Dans les premiers jours du Barreau, les conseillers en nommaient d'autres selon les besoins. Ce mode de nomination des nouveaux conseillers a donné lieu à une profession étroitement contrôlée de l'intérieur. En 1871, le gouvernement a adopté une loi qui mettait fin aux nominations à vie et qui donnait à tous les membres en règle du Barreau le droit de voter pour les 30 conseillers qui devaient remplir des mandats de cinq ans (à l'exception de certains conseillers qui avaient été nommés à leur poste par une instance politique). Toutefois, la législation n'a pas changé le droit des conseillers de nommer qui ils voulaient afin de remplir les postes qui étaient devenus vacants pendant le mandat de cinq ans. L'année 1912 a vu la création des conseillers à vie. Les conseillers à vie étaient des conseillers qui obtenaient des nominations permanentes après avoir été élus un certain nombre de fois. Les conseillers à vie gardaient le droit de voter, mais on ne les comptait pas dans les 30 conseillers élus.

La *Loi sur la Société du barreau* (*Law Society Act* (LSA)) a été adoptée en 1970. Le nombre de conseillers est passé à 40. Le mandat traditionnel de cinq années est devenu un mandat de quatre ans. La représentation régionale a été mise en œuvre. Les postes vacants pendant le mandat de cinq ans seraient remplis par les candidats défaits d'après le nombre de votes reçus. Des dispositions sur les enquêtes et les mesures disciplinaires à imposer aux membres ont été ajoutées. Pour la première fois, quatre postes de conseillers non juristes nommés par le gouvernement ont été créés (actuellement, ce chiffre s'élève à huit). La Loi exigeait une réunion générale annuelle. La Loi a été révisée en 1998 et on a modifié la représentation régionale pour mieux refléter la représentation provinciale.

7.5.3 Gouvernance actuelle

Afin de remplir son mandat, le Barreau met en œuvre un certain nombre de programmes d'enseignement et d'information de ses membres. Le Barreau mène des vérifications ponctuelles afin de mesurer l'intégrité des déclarations financières des firmes d'avocats et de s'assurer que les praticiens du droit respectent les exigences de tenue des dossiers. Ces vérifications ponctuelles visent à identifier et à corriger rapidement les petits problèmes avant qu'ils ne deviennent des problèmes graves de non-conformité ou d'inconduite.

Le Barreau régit la communauté juridique de l'Ontario en partie grâce à ses Règles de conduite professionnelle, soit le Code de déontologie (les Règles). Ces Règles établissent les obligations professionnelles et éthiques de tous les membres du Barreau. Les premières « Règles » ont paru en 1964. À la suite de leur entrée en vigueur le 1er novembre 2000, les nouvelles Règles ont été continuellement modifiées afin de mieux servir à la fois les avocats et le public. Par exemple, le Barreau envisage actuellement une modification visant à inclure une nouvelle règle concernant le conflit d'intérêt dans le contexte d'une relation sexuelle entre un avocat (ou une avocate) et le client (ou la cliente). Le Barreau publie des avis en matière de pratique afin d'aider les membres à mieux comprendre les Règles et la gestion de la pratique. Pour l'instant, les Règles sont regroupées en six catégories qui traitent de différents domaines ou de différents aspects de la pratique tels que la relation de l'avocat avec les clients, la façon d'éviter les conflits d'intérêt et la relation de l'avocat avec l'administration de la justice.

En outre, il y a d'autres divisions dans le Barreau ainsi que d'autres organisations qui servent à aider les avocats et à garder l'intégrité de la profession juridique :

Fonds d'assurance responsabilité civile professionnelle (Lawyers Fund for Compensation)
Ce fonds aide les clients qui ont perdu de l'argent à cause de la conduite malhonnête d'un avocat. Il est financé uniquement par les avocats et par leurs ressources personnelles. Depuis ses débuts, le fonds a versé des millions de dollars. La majorité des pertes des clients sont le fait d'avocats qui ont détourné des fonds en fidéicommis.

Lawyer's Professional Indemnity Company (LawPro)
Avec son siège social à Toronto et incorporée par le Barreau en 1990, LawPro est une compagnie d'assurance indépendante qui a le permis d'assurance de responsabilité civile et l'assurance de titres dans les juridictions partout au Canada.

Aide juridique Ontario (Legal Aid Ontario)
La *Loi sur les services juridiques* a établi l'Aide juridique Ontario en 1998. L'aide juridique a pour principal mandat de « favoriser l'accès à la justice, partout en Ontario, des personnes à faible revenu en assurant uniformément des services d'aide juridique de grande qualité de manière rentable et efficace »[125].

[125] *Loi sur les services juridiques (Legal Aid Services Act), 1998*, S.O. 1998, c. 26, section 1.

7.5.4 La procédure de sanctions disciplinaires

La procédure en cours au Barreau pour traiter les plaintes est semblable à celle qui est adoptée par d'autres corps dirigeants professionnels comme ceux des docteurs et des dentistes. La procédure est établie dans la *Loi sur la Société du barreau* et elle comprend diverses étapes quant à l'examen des plaintes, aux audiences, aux appels et à l'examen par les tribunaux.

Les membres peuvent être suspendus par certains conseillers élus pour des violations administratives comme le fait de ne pas payer les frais annuels ou de ne pas faire les déclarations annuelles. L'avocat ne peut pas exercer le droit tant que la suspension est en cours. Les motifs de plainte contre un avocat comprennent ce qui suit : inconduite professionnelle, conduite inconvenante de la part d'un avocat ou d'un procureur, incapacité, incompétence, cotisations non payées, déclarations non faites et audience de bonne moralité pour l'admission des membres.

Le Barreau reçoit des plaintes contre des avocats de plusieurs sources, y compris les clients, d'autres avocats, les tribunaux, la police ou le grand public. Après réception de la plainte, le Barreau informe en général le membre et lui donne la possibilité de répondre. Les avocats ont l'obligation de répondre rapidement. Le fait de ne pas répondre rapidement constitue un motif de sanction disciplinaire. L'infraction mineure est envoyée à division de règlement des plaintes du Barreau. L'infraction plus grave est transmise à la division des enquêtes. Les deux divisions font partie du service de la réglementation professionnelle du Barreau.

Le commissaire chargé du règlement des plaintes les examine et essaie de régler les plaintes des personnes qui ne sont pas satisfaites avec le règlement initial du Barreau. Si la plainte n'est toujours pas réglée de manière satisfaisante, elle peut être envoyée au Comité d'autorisation de la procédure. Ce comité peut autoriser la tenue d'une audience devant un groupe de trois conseillers. Le comité d'audience a le pouvoir de rendre une ordonnance en vertu de la *Loi sur la Société du barreau* (réprimande, radiation du tableau de l'ordre, suspension ou amende). L'audience ressemble beaucoup à celle d'un tribunal, mais elle est moins formelle. Par exemple, on peut y accepter les preuves par ouï-dire.

On peut interjeter appel des décisions du comité d'audience auprès d'un comité d'appel composé de sept conseillers. Un appel de la décision du comité d'appel peut être fait devant la cour divisionnaire. On peut interjeter appel des décisions de la cour divisionnaire devant la Cour d'appel de l'Ontario ou devant la Cour suprême du Canada.

7.5.5 Autres règles et lois de gouvernance

Outre les Règles (ou Code de déontologie) et les divers règlements dans le cadre de la *Loi sur la Société du barreau*, le Barreau a adopté les Règles de pratique et de procédure pour les audiences de sanctions disciplinaires. Ces règles gouvernent la conduite des audiences devant un comité d'audience ou un comité d'appel et elles servent de supplément à la *Loi sur l'exercice des compétences légales* qui régit les tribunaux administratifs de l'Ontario. La *Loi sur les procureurs* traite des questions comme celles de la pratique non autorisée du droit en Ontario et de l'évaluation des coûts d'un procureur.

7.5.6 Les résultats

Comme la profession se réglemente et se gouverne, il faut absolument avoir des mécanismes pour s'assurer que la profession juridique maintient un niveau élevé de service et d'éthique. Les barreaux partout au pays ont répondu à cette exigence en mettant en œuvre des programmes, des règles, des systèmes de responsabilité et des moyens qui, mis ensemble, assurent le maintien de normes élevées. En cas de violation d'une norme, il y a un certain nombre de systèmes en place pour régler et résoudre efficacement cette violation. Les structures actuelles de responsabilité sont justes, souples et rapides. Les barreaux ont depuis longtemps montré leur volonté de s'adapter et de réagir aux changements afin de s'assurer qu'ils ne répondent pas tout simplement aux besoins juridiques de la société, mais qu'ils vont bien au-delà.

7.5.7 Leçons en matière de responsabilité

Les divers participants dans le secteur ont offert les opinions suivantes concernant les leçons en matière de responsabilité :

- Pour que les entités autoréglementées aient de la crédibilité aux yeux du public, elles doivent assurer une procédure de responsabilité transparente, efficace, significative et souple;
- La confiance du public dans l'entité autoréglementée a une importance primordiale;
- Pour que le public ait véritablement confiance dans l'organisme et le système d'autoréglementation, il vaut mieux mettre en place des mécanismes de responsabilité bien définis et applicables;
- La mise en œuvre de systèmes (comme le Fonds d'assurance responsabilité civile professionnelle) qui offrent des niveaux additionnels de soutien et de redressement lorsque les choses vont mal aide à inspirer de la confiance dans l'entité autoréglementée et
- Les entités autoréglementées doivent mettre à jour et adapter de façon diligente les normes de responsabilité à mesure que les environnements de responsabilité évoluent.

7.6 Leçons en matière de responsabilité dans l'infrastructure d'information essentielle

Les opinions des participants du secteur au sujet des leçons en matière de responsabilité sont présentées dans quelques-unes des sections précédentes. Dans cette section, nous présentons des moyens selon lesquels ces leçons *peuvent* s'appliquer à l'infrastructure d'information essentielle. Cela pourrait s'avérer intéressant.

7.6.1 Services de santé et services juridiques

Les professions sont le plus en mesure de définir des normes et des certifications pour leurs membres et d'assurer l'adhésion à ces normes et certifications. La menace constante de la réglementation assure l'intégrité. Les normes et certifications professionnelles peuvent être nécessaires si nous voulons atteindre un niveau de responsabilité significatif dans l'infrastructure d'information essentielle.

7.6.2 Services financiers

Les environnements dynamiques requièrent des modèles adaptables de responsabilité avec un processus d'évolution intégré afin d'assurer leur pertinence et leur efficacité. Il y a peu d'environnements plus dynamiques que celui de l'infrastructure d'information.

Une responsabilité efficace dépend de normes claires de mesure. L'infrastructure d'information essentielle n'a pas un bon nombre des normes nécessaires à l'application de la responsabilité. Bien des gens estiment que de telles normes devraient être établies.

Dans les situations où les organisations ne contrôlent pas tout l'environnement, il est logique de les tenir responsables des processus bien définis suivants. L'infrastructure d'information essentielle est un ensemble de parties interdépendantes sans aucun contrôle centralisé. La responsabilité en matière de processus par rapport à la responsabilité en matière de résultats peut être, en général, plus applicable.

7.6.3 Services d'électricité

La responsabilité en matière de résultats aux interfaces entre les systèmes privés et le système partagé a du sens. Les interfaces offrent un point défini de mesure. L'infrastructure d'information essentielle se compose de nombreux systèmes privés qui ont une interface avec un vaste système partagé. Les exploitants des systèmes privés peuvent être tenus responsables si jamais ils « exportent les problèmes » vers le système partagé.

8.0 Initiatives en matière de responsabilité

Dans la section 7, nous traitons de l'évolution du concept de responsabilité dans d'autres environnements et de quelques-unes des leçons apprises. Au fur et à mesure de nos recherches dans ces environnements, nous avons découvert un certain nombre d'initiatives spécifiques et intéressantes en matière de responsabilité. Chacune de ces initiatives a également quelques leçons à nous offrir. Elles peuvent nous inspirer pour ce qui est de régler la question de la responsabilité dans l'infrastructure d'information essentielle. Dans cette section, nous présentons de brefs résumés de ces initiatives et nous concluons en discutant de leur pertinence dans le domaine de l'infrastructure d'information essentielle.

8.1 An 2000

8.1.1 Le problème

Les systèmes informatiques devaient faire face à un problème qui risquait d'être grave en relation avec l'année 2000 (Y2K) – le fameux Problème An 2000[126]. Ce problème était dû au fait que l'on avait pensé que deux chiffres étaient suffisants pour représenter l'année de n'importe quelle date; ainsi « 03/21/39 » était universellement accepté comme l'expression abrégée de « 21 mars 1939 ». Presque tous les programmes informatiques bâtis dans les années 1960 et 1970 et de nombreux programmes des années 1980 ont utilisé cette abréviation[127] pour les dates. Lorsque les ordinateurs exécutaient des opérations arithmétiques sur ces dates abrégées, tout marchait bien, à condition que les dates se situent entre le 1er janvier 1900 et le 31 décembre 1999.

Les auteurs d'un bon nombre de ces programmes écrits dans les années 1960, 1970 et 1980 croyaient que la durée de vie de leurs programmes serait inférieure à dix ans. Il pourrait y avoir des problèmes en 2000, mais ils étaient pratiquement sûrs que les premiers programmes seraient remplacés bien avant le 1er janvier 2000. Cela ne s'est pas passé tout à fait de cette façon. Bien des programmes encore actifs en 1995 ne pouvaient plus traiter correctement les dates après le 1er janvier 2000. Il y avait un véritable problème technique An 2000 dans de nombreux systèmes informatiques. Si le problème n'était pas corrigé, beaucoup de ces systèmes informatiques risquaient de tomber en panne.

[126]Une quantité considérable d'information au sujet du Problème An 2000 était accessible sur l'Internet. Un bon nombre des sites An 2000 les plus populaires ne sont plus en ligne puisqu'il n'y avait plus de raison de maintenir leur présence. Quelques-uns des sites ont été maintenus, le plus souvent dans le cadre de la présence d'une organisation permanente sur l'Internet. L'IEE de la Grande-Bretagne a un tel site – voir en ligne <http://www.iee.org/Policy/Areas/Y2K/index.cfm>. Le Service d'extension de l'Oregon State University tient un site Web d'archivage étendu sur l'An 2000 (Y2K) à <http://extension.oregonstate.edu/archives/y2k/index.html>.

[127]En Amérique du Nord, il était courant d'avoir une représentation interne de la date comme une chaîne de six chiffres, par exemple le 21 mars 1930 s'écrivait 032139. Il y avait des programmes standard pour calculer le nombre de jours, de semaines, de mois et d'années entre deux dates (par exemple, le programme calculait que 032140 venait 365 jours après 032139).

8.1.2 La réponse

Vers les années 1990, un certain nombre de personnes ont reconnu que nous allions faire face à un problème informatique de l'An 2000. Il y avait déjà eu plusieurs articles et discours sur le sujet. Très peu de mesures ont été prises assez tôt pour même comprendre le problème; nous ne savions pas véritablement quels systèmes informatiques étaient les plus vulnérables ni même les conséquences probables des pannes d'ordinateurs en l'An 2000. Cette section du rapport donne une histoire anecdotique[128] du Problème An 2000 et suggère comment quelques-unes des connaissances acquises peuvent s'appliquer (ou non) aux efforts de maintien de notre infrastructure d'information essentielle.

Presque tous ceux qui travaillaient dans le domaine informatique savaient que nous devions faire face à un problème de l'An 2000. Ils ne s'entendaient tout simplement pas sur l'étendue et la gravité de ce problème. Mais peu de gestionnaires dans le domaine des TI se sont avancés pour prendre la responsabilité ou accepter l'obligation de rendre des comptes. En un sens, c'était une réaction humaine naturelle à un problème qui n'était pas urgent. Au début des années 1990, il y avait encore de nombreuses années avant que les problèmes de l'An 2000 ne fassent surface. Des problèmes plus immédiats exigeaient l'attention.

On réalisait très peu de progrès en parlant avec les gestionnaires des TI, mais il y avait une montée constante de la pression du public à ce sujet. Le problème de l'An 2000 était mûr pour le traitement dans la presse populaire et d'affaires. Le problème était relativement facile à décrire et les scénarios de catastrophe semblaient fortement plausibles. Vers le milieu des années 1990, la pression se faisait de plus en plus sentir pour que des mesures soient prises.

Lorsque la question en est arrivée à un point critique, c'était largement inspiré par le sentiment de devoir couvrir ses arrières (en anglais, on utilisait l'euphémisme CYA[129]). Les gestionnaires, particulièrement les cadres supérieurs, ne voulaient pas avoir l'air passifs devant un problème qui était clair et évident pour les entreprises et le gouvernement. En 1997-1998, la plupart des grandes institutions, particulièrement les principaux établissements financiers, étaient bien en voie de régler leurs problèmes An 2000. On passait de la question « qu'allons-nous faire au sujet de l'An 2000? » à la question « qu'avez-vous fait au sujet du problème de l'An 2000? ». Il y avait aussi une préoccupation croissante au sujet du problème et cela s'exprimait sous forme de déclarations au sujet des obligations fiduciaires des directeurs, des cadres supérieurs et des conseillers professionnels.

Les principales banques se préoccupaient de savoir si leurs clients d'affaires avaient pris les mesures appropriées pour régler les problèmes de l'An 2000. Les vérificateurs admettaient qu'ils avaient la responsabilité professionnelle de soulever les questions de préparation à l'An 2000.

---

[128]Nous avons eu la chance d'avoir une entrevue téléphonique avec Peter de Jaeger le 2 mars 2004. M. de Jaeger était l'un des champions les plus visibles du Problème An 2000 dans le milieu anglophone. Son site Web An 2000, <http://www.year2000.com/>, était l'un des plus actifs à fournir une vaste gamme de renseignements sur le sujet. Son site Web actuel (<http://www.technobility.com/>) donne l'information complète au sujet de ses activités en cours. L'information donnée dans cette section provient essentiellement de la conversation avec Peter de Jaeger. Elle est également fondée, en partie, sur l'expérience pratique de Mark Stirling et de Robert Fabian, deux des participants au présent rapport.

[129]Souvent traduit poliment par « Cover Your Assets ».

Les avocats commençaient à signaler à leurs clients qu'ils pouvaient subir de sérieuses menaces sur le plan juridique en vertu des principes des lois commerciales et de la négligence si des mesures appropriées n'étaient pas prises pour régler les problèmes de l'An 2000. Les fournisseurs demandaient de plus en plus des déclarations de conformité à l'An 2000. Chacun des « partenaires » d'affaires voulait avoir des déclarations de conformité An 2000 des autres partenaires. Les banques exigeaient des déclarations de conformité An 2000 de la plupart de leurs clients d'affaires. À la fin, il y avait des affaires florissantes grâce à l'An 2000[130].

Le problème de l'An 2000 était un bon exemple d'une question de responsabilité « simple » :

- Le problème était *facile à comprendre*;
- Il y avait une *date limite fixe* et
- Les *solutions* techniques étaient connues.

8.1.3 Les résultats

La pression sociale était assez forte pour que la société consacre ce qu'il fallait pour résoudre le problème de l'An 2000[131]. Il y a eu relativement peu de pannes liées à l'An 2000. Dans la plupart des cas, des solutions de rechange faciles ont été déployées (par exemple, une lettre qui demandait aux clients de ne pas tenir compte de l'impression incorrecte de « 1900 » dans un état financier lorsqu'il aurait fallu avoir « 2000 »). Collectivement, nous avons vraiment résolu le problème de l'An 2000.

Toutefois, le point central de la solution a été l'application de forces sociales de la part des conseils d'administration, des « partenaires » d'affaires et des conseillers professionnels. La responsabilité n'a pas été facilement acceptée par ceux qui avaient les connaissances et les compétences requises pour résoudre le problème.

8.2 La Commission Treadway

8.2.1 Le problème

La National Commission on Fraudulent Financial Reporting a été fondée en 1985 aux États-Unis. Elle était plus couramment connue sous le nom de Treadway Commission (TC) d'après son président, James C. Treadway Jr. La TC jouissait du parrainage conjoint dans le secteur privé des organismes suivants : Financial Executives International, American Accounting Association, American Institute of Certified Public Accountants, Institute of Internal Auditors et Institute of Management Accountants. La Commission avait pour mandat d'inspecter les rapports financiers, de les analyser et de faire des recommandations sur l'information financière frauduleuse des sociétés ouvertes. Après avoir étudié pendant deux ans le système de rapports financiers, la TC a publié un rapport (le Rapport). Le but déclaré de la TC était « d'identifier les

[130]Les membres du public avaient beaucoup d'appréhension. La vente des génératrices a augmenté. Les gens ont stocké de l'eau en bouteille et des boîtes de conserve. La presse populaire a offert toutes sortes de conseils au sujet de ce qu'il fallait faire au moment de la catastrophe de l'An 2000. C'était une époque frénétique.

[131]On pourrait avancer qu'en tant que société, nous dépensons trop pour les solutions. On a certainement demandé et publié une masse énorme de déclarations de conformité An 2000 à mesure que le 1er janvier 2000 approchait.

facteurs qui peuvent être la cause de rapports financiers frauduleux et de déterminer les étapes visant à réduire leur incidence »[132].

L'introduction du Rapport déclare :

> L'information financière frauduleuse est véritablement un grave problème. Même si on prétend qu'elle est peu fréquente, ses conséquences peuvent être généralisées et importantes. Même s'il est difficile de prévenir la fraude sous une forme quelconque, on peut réduire l'information financière frauduleuse, de manière substantielle peut-être, si chaque partie à laquelle nous avons fait des recommandations prend les mesures que nous recommandons[133].

8.2.2 La réponse

La TC avait trois objectifs importants :

> (1) Envisager dans quelle mesure les actes menant à de l'information financière frauduleuse minent l'intégrité de l'information financière; considérer les forces et les possibilités ainsi que les facteurs environnementaux, institutionnels ou individuels qui peuvent contribuer à ces actes; voir dans quelle mesure on peut prévenir ou éviter l'information financière frauduleuse et comment la détecter plus rapidement après son apparition; examiner dans quelle mesure, le cas échéant, les incidents de ce type de fraude peuvent être le produit du déclin du professionnalisme chez les cadres financiers de l'entreprise et les vérificateurs internes et, dans quelle mesure, le cas échéant, le cadre de réglementation et d'application de la loi a pu involontairement tolérer ce type de fraude ou contribuer à son apparition.
>
> (2) Examiner le rôle de l'expert-comptable indépendant dans la détection de la fraude et se concentrer particulièrement sur le fait de savoir si la détection de l'information financière frauduleuse a été négligée ou insuffisamment ciblée et si la capacité de l'expert-comptable indépendant à détecter une telle fraude peut être améliorée; considérer également si des changements apportés aux normes ou aux procédures de vérification (internes et externes) réduiraient l'étendue de l'information financière frauduleuse.
>
> (3) Déterminer les attributs de la structure d'entreprise qui peuvent contribuer à des actes menant à de l'information financière frauduleuse ou à l'absence de détection appropriée de tels actes[134].

Le Rapport se divise en cinq chapitres :

1. Aperçu du système de rapports financiers et de l'information financière frauduleuse;
2. Recommandations pour la société ouverte;
3. Recommandations pour l'expert-comptable indépendant;
4. Recommandations pour la SEC et pour d'autres organismes afin d'améliorer le cadre de réglementation et le cadre juridique et
5. Recommandations pour l'éducation.

---

[132] « Treadway Commission Report on Fraudulent Financial Reporting » [The Report].
[133] *Ibid*. à 2.
[134] *Ibid*. à 2.

La TC a observé que « puisque les rapports financiers des sociétés ouvertes constituent l'élément le plus critique d'une divulgation complète et équitable qui assure le fonctionnement efficace des marchés de capitaux et de crédits aux États-Unis … notre examen nous a menés à conclure qu'il faut prendre des mesures pour améliorer notre système de rapports financiers, en dépit de son excellence actuellement »[135]. La TC a conclu ce qui suit :

- « Aucune compagnie, quelles que soient la taille ou les affaires, n'est protégée contre la possibilité d'une information financière frauduleuse. Cette possibilité est inhérente à la conduite des affaires[136];
- « La nature multidimensionnelle du problème devient claire lorsque nous considérons simplement les nombreux participants qui façonnent le processus de rapports financiers … Chacun d'eux a la possibilité d'influer sur les résultats …[137];
- « La responsabilité de rapports financiers fiables se trouve d'abord et avant tout au niveau de l'entreprise …la [r]éduction du risque de rapports financiers frauduleux doit d'abord avoir lieu dans la compagnie même[138].
- « L'une des pratiques clés [pour aider toutes les sociétés ouvertes à remplir leurs responsabilités et à réduire l'incidence d'une information financière frauduleuse] est celle de la constitution par le conseil d'administration d'un comité de vérification informé, vigilant et efficace qui surveillera le processus des rapports financiers de la compagnie. Une autre pratique vise à établir et à maintenir une fonction de vérification interne[139].
- « Les experts-comptables indépendants jouent un rôle crucial, mais secondaire. Ils ne sont pas garants de l'exactitude ou de la fiabilité des états financiers[140].
- « Les organismes de réglementation et d'application de la loi fournissent le moyen de dissuasion qui est essentiel à la réduction de l'incidence de rapports financiers frauduleux … Mais des améliorations peuvent et devraient être faites, à la fois au niveau fédéral et à celui de l'État[141].
- « L'éducation peut préparer les étudiants en comptabilité et en administration à reconnaître les facteurs qui peuvent contribuer à ce type de fraude ainsi que les valeurs éthiques et les bonnes pratiques d'affaires qui sont nécessaires pour se protéger contre la fraude. »

8.2.3 Les résultats

Même si le Rapport a été bien reçu, une personne cynique pourrait résumer l'impact de la TC par un seul mot : Enron. Du côté positif, le Rapport a été extrêmement utile puisqu'il a permis d'identifier les divers participants à la « chaîne alimentaire » des rapports financiers. Il a également fait des recommandations importantes qui pourraient jouer un rôle considérable pour ce qui est de minimiser les possibilités d'une information financière frauduleuse. Toutefois, on doit souligner que le mandat de la TC était de faire des recommandations. Sans mise en œuvre,

[135] *Ibid*. à 5.
[136] *Ibid*. à 6.
[137] *Ibid.*
[138] *Ibid*.
[139] *Ibid*.
[140] *Ibid*.
[141] *Ibid*.

même la meilleure recommandation se retrouve dans le cimetière des bonnes intentions. Pendant les années intermédiaires, de nombreuses études et beaucoup de groupes de recherche ont été radiés afin de bâtir sur le travail entrepris par la TC. Avec l'arrivée de la loi *Sarbanes-Oxley Act of 2002*, quelque 14 ans après la diffusion du Rapport, un bon nombre des recommandations de la TC ont été finalement mises en œuvre.

8.3 La loi Sarbanes-Oxley Act of 2002

8.3.1 Le problème

La compagnie Enron s'est effondrée à cause d'une fraude d'entreprise. Arthur Andersen a été reconnu coupable d'obstruction à la justice dans l'enquête sur Enron. Face à des accusations selon lesquelles sa recherche sur les actions avait trompé les investisseurs, Merrill Lynch a accepté de verser une amende de 100 millions de dollars US afin que les accusations soient retirées en échange. Les répercussions des fraudes continuent à mesure que la portée des enquêtes s'élargit. WorldCom s'est écrasée à cause d'une fraude comptable de 11 milliards de dollars US. Avec cet assaut de scandales, l'intervention législative qui visait à définir les normes de l'entreprise et à tenir responsables ceux qui violaient ces normes n'était pas loin derrière. Le sénateur Paul Sarbanes (D-Maryland) a déclaré ce qui suit : « Il faut faire quelque chose pour restaurer la confiance dans le plus grand marché au monde. » Ce « quelque chose » est venu sous la forme de la *Sarbanes-Oxley Act of 2002* (SOA).

8.3.2 La réponse

La SOA a été nommée d'après ses deux partisans au Congrès, soit le sénateur Paul Sarbanes et le représentant Michael Oxley (R-Ohio). La SOA est entrée en vigueur aux États-Unis le 30 juillet 2002 et elle définit son mandat comme suit : « Loi qui vise à protéger les investisseurs en améliorant l'exactitude et la fiabilité des divulgations de l'entreprise faites en vertu des lois sur les valeurs mobilières et à d'autres fins[142]. » À la signature de la SOA en tant que loi, le président des États-Unis George W. Bush a lancé une mise en garde à l'Amérique des entreprises en déclarant que « chaque cadre de l'entreprise qui a choisi de commettre un crime peut s'attendre à faire face aux conséquences de ce crime ».

La SOA comprend onze titres qui, ensemble, visent ce qui suit :

- Renforcer la responsabilité de l'entreprise et la gouvernance des sociétés ouvertes,
- Avoir un impact sur les directeurs et les cadres,
- Rendre les vérificateurs plus indépendants et soumis à des normes d'intégrité et de contrôle de la qualité,
- Habiliter des comités de vérification,
- Établir des mesures de protection pour les dénonciateurs,
- Traiter des conflits d'intérêt dans le cas des analystes en valeurs mobilières et
- Offrir des mesures de protection contre la fraude aux employés, aux détenteurs des pensions et aux investisseurs.

[142] *Sarbanes-Oxley Act of 2002*.

La SOA crée le conseil indépendant Public Company Accounting Oversight Board (le Conseil) pour agir en tant qu'organisme qui surveille la vérification des sociétés ouvertes soumises aux lois sur les valeurs mobilières. Le Conseil protège les intérêts des investisseurs dans la préparation de rapports de vérification exacts et indépendants et supervise l'industrie de la comptabilité, sous la direction de la SEC (Securities and Exchange Commission ou Commission des opérations de Bourse) qui gouverne les opérations sur les valeurs mobilières. On a octroyé une plus grande indépendance aux vérificateurs par rapport à leurs clients des sociétés ouvertes en les empêchant de fournir certains services qui n'avaient pas trait à la vérification. Les firmes de vérification doivent faire maintenant le roulement entre le principal partenaire de vérification et le partenaire responsable de l'examen de la vérification afin qu'aucun des deux ne remplisse le même rôle de vérification pendant plus de cinq années consécutives.

Chaque société ouverte doit avoir un comité de vérification. Chaque membre du comité de vérification doit être un membre du conseil d'administration de la compagnie, il ne doit pas accepter d'autre rémunération que celle de membre du comité de vérification et il ne doit avoir aucune autre affiliation avec la compagnie. Les vérificateurs ne font rapport qu'au comité de vérification et non à la direction. La SOA donne comme mandat aux sociétés ouvertes de créer des systèmes permettant aux employés de signaler les inconduites (c'est-à-dire de « vendre la mèche »). Les comités de vérification doivent mettre en œuvre des procédures pour la réception, la conservation et le règlement des plaintes, y compris le signalement confidentiel et anonyme d'affaires douteuses de vérification, de contrôles comptables internes et de comptabilité. Les « dénonciateurs » qui subissent des mesures de représailles de la part de leurs employeurs peuvent maintenant déposer des griefs devant le Department of Labor et les tribunaux de district des États-Unis. En vertu de la SOA, les représailles constituent une infraction à la loi fédérale qui est punissable par un emprisonnement maximal de dix ans.

En vertu de la SOA, la responsabilité quant aux états financiers et autres divulgations d'une société ouverte incombe véritablement aux cadres supérieurs et le président-directeur général ainsi que le directeur financier doivent personnellement certifier les divulgations faites dans les rapports périodiques. Selon la SOA, toute violation de cet article à caractère volontaire ou délibéré est un acte délictueux grave qui est punissable par un emprisonnement maximal de 20 ans.

Les cadres supérieurs et les administrateurs des sociétés ouvertes doivent signaler leurs opérations personnelles sur les valeurs mobilières de la compagnie dans les deux jours ouvrables, ce qui réduit énormément la période de rapport qui était auparavant de 40 jours au maximum. Leurs opérations doivent être affichées dans le site Web de la compagnie. Les initiés qui violent cet article peuvent être poursuivis par la compagnie et leurs profits seraient remboursés à la compagnie. Si une société doit redresser ses états financiers à la suite d'une inconduite, le président-directeur général et le directeur financier doivent rembourser à la compagnie les bonus ou autres formes de rémunération reçus pendant la période de 12 mois qui suivait la première émission publique ou le dépôt auprès de la SEC du document financier.

Les sociétés ouvertes doivent indiquer si un code d'éthique a été adopté pour les cadres financiers et, si ce n'est pas le cas, elles doivent expliquer pourquoi. La SOA interdit des prêts personnels des sociétés ouvertes à leurs cadres supérieurs et administrateurs s'ils ne sont pas faits dans le cours ordinaire des affaires. Les délais pour signaler de l'information négative possible

sont améliorés. La SOA donne des lignes directrices aux analystes en valeurs mobilières afin d'assurer des avis impartiaux. Le secret professionnel est redéfini dans le cas des avocats qui représentent les clients de sociétés ouvertes. Les avocats de l'extérieur qui représentent les sociétés ouvertes doivent prendre les mesures appropriées lorsqu'ils découvrent des preuves d'actes fautifs, en dépit de la vieille règle selon laquelle les communications entre un avocat et son client sont confidentielles. Par exemple, ces avocats doivent divulguer leurs constatations au président-directeur général ou à l'avocat-conseil de la compagnie et ils doivent s'assurer que ces divulgations sont traitées de la façon appropriée par ces représentants de la compagnie. Si tel n'est pas le cas, les avocats ont l'obligation de faire rapport à un comité de vérification de la compagnie, à des administrateurs indépendants ou à des conseils d'administration. Si les mesures appropriées ne sont toujours pas prises, l'avocat doit en informer la SEC.

La SOA crée un certain nombre de sanctions civiles et pénales qui favorisent la conformité. Par exemple, la destruction, la modification ou la falsification de dossiers ou de documents dans le but de gêner, d'entraver ou d'influencer une enquête fédérale sont punissables par une amende et/ou par un emprisonnement maximal de 20 ans.

8.3.3 Les résultats

La SOA vise essentiellement à offrir aux organismes de réglementation en valeurs mobilières et d'application de la loi les outils nécessaires pour arrêter la criminalité en col blanc perpétrée par les personnes mêmes qui sont chargées de faire fonctionner l'Amérique des entreprises. La SOA réalise cela en établissant des normes de comportement et en offrant des mécanismes pour tenir responsables les personnes qui violent ces normes. Étant donné que la SOA n'a pas tout à fait deux ans, il est peut-être trop tôt pour bien juger de son impact. En outre, le fait d'avoir des outils pour combattre un problème et l'utilisation de ces outils constituent deux éléments distincts, tout comme le fait d'avoir des politiques et de les mettre en œuvre sont deux choses distinctes. Toutefois, la création de la richesse et d'une économie stable et croissante grâce à l'investissement dans les sociétés ouvertes est perçue comme l'un des piliers du système économique américain. Le système d'investissement est menacé d'effondrement si ceux qui ont utilisé traditionnellement ce système estiment qu'ils ne peuvent plus lui faire confiance. Peut-être que la seule façon de s'assurer que le mode de vie des Américains continuera à prospérer, c'est de restaurer la confiance du public dans ce système en persuadant un public blasé que des mesures législatives appropriées sont en place, que les autorités veulent utiliser les outils fournis par la nouvelle législation et qu'il y a de véritables conséquences pour ceux qui sont déclarés coupables de fraude économique.

8.4 Directives de l'Union européenne sur la protection des données à caractère personnel

8.4.1 Le problème

La formation de l'Union européenne (UE) a fortement augmenté la nécessité de transférer les données personnelles au sein de l'Union. En même temps, il y avait une sensibilité croissante du public quant à la nécessité de préserver la confidentialité de ces données. Les exigences en matière de responsabilité dans la collecte, l'utilisation, la conservation et la divulgation des données personnelles ont augmenté avec le développement d'énormes bases de données informatisées.

8.4.2 La réponse

La directive de l'Union européenne sur la protection des données à caractère personnel[143] a été promulguée dans le but de fournir un cadre de réglementation qui permettrait le libre transfert de l'information personnelle entre les pays membres de l'Union européenne. De plus, cela devait assurer un niveau minimal de sécurité de l'information, que celle-ci soit stockée, transmise ou traitée.

La Directive s'applique au « traitement » des « données à caractère personnel ». Les données à caractère personnel représentent « toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »[144]. Le traitement des données est « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction »[145].

Afin que le traitement des données à caractère personnel soit légitime en vertu de la Directive, celui qui recueille les données personnelles doit divulguer, au moment de la collecte, son identité, les buts spécifiques de la collecte des données et tous les destinataires des données recueillies. La collecte doit se limiter aux données qui sont nécessaires aux fins d'identification. Les données ne peuvent être conservées que pendant la période de temps qui est nécessaire à ces fins.

Les données à caractère personnel ne peuvent être traitées aux fins identifiées que si la personne concernée a donné son consentement « sans ambiguïté ». Elle doit être informée de la divulgation des données à caractère personnel à des tiers et elle doit avoir le droit de refuser. On doit garantir aux personnes le droit d'accès et le droit de demander des modifications dans le cas de données inexactes. Le responsable de la collecte des données doit surveiller l'exactitude des données et les corriger au besoin. Des règles plus strictes s'appliquent au traitement des données sensibles (par exemple, sur la santé ou la vie sexuelle)[146].

Des tiers peuvent exécuter le traitement des données mais ils doivent être régis par un contrat qui stipule que le « sous-traitant n'agit que sous la seule instruction du responsable du traitement »[147]. « Le responsable du traitement doit mettre en œuvre les mesures techniques et

[143]Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, [1995] O.J. L. 281/31, [« Directive »].
[144]Directive, Article 2(a).
[145]Directive, Article 2(b).
[146]Directive, Article 8.
[147]Directive, Article 17(3).

d'organisation appropriées pour protéger les données à caractère personnel[148]. » À son tour « le responsable du traitement, lorsque le traitement est effectué pour son compte, doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité techniques et d'organisation relatives aux traitements à effectuer et il doit veiller au respect de ces mesures[149]. » La Directive n'exige pas que la personne concernée donne un consentement distinct pour le recours à un tiers.

8.4.3 Les résultats

On s'entend généralement pour dire que la Directive a été un succès. Elle a été essentielle à la mise en œuvre d'une protection de base de l'information personnelle qui est recueillie et traitée au cours des activités commerciales.

Ses effets ne se sont pas limités à l'Union européenne. Le transfert de données à un sous-traitant situé dans un pays en dehors de l'Union européenne est permis lorsque ce pays assure un « niveau adéquat de protection » des données. Le 20 décembre 2001, la Commission a décidé que le Canada est considéré comme un pays qui fournit un niveau adéquat de protection des données personnelles transférées à partir de l'Union aux destinataires assujettis à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ/PIPEDA)[150].

En fait, la LPRPDÉ a été mise en œuvre, en partie, pour répondre aux exigences de la Directive. D'autres pays ont également agi de la même façon pour que le transfert légitime des données personnelles puisse se poursuivre avec les membres de l'Union européenne.

8.5 La *Loi sur la protection des renseignements personnels et les documents électroniques*

8.5.1 Le problème

L'expérience au Canada reflète l'expérience à l'Union européenne. L'information personnelle est devenue un bien extrêmement lucratif qui est constamment transféré à mesure que les gens exécutent des opérations quotidiennes et de routine. Le gouvernement du Canada a essayé de répondre aux préoccupations du public au sujet de la collecte, de l'utilisation, de la conservation et de la divulgation de l'information personnelle en mettant en œuvre la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ/PIPEDA)[151].

[148]Directive, Article 17(1).
[149]Directive, Article 17(2).
[150]Décision de la Commission du 20 décembre 2001, en vertu de la Directive 95/46/EC du Parlement européen et du Conseil sur la protection adéquate des données à caractère personnel assurée par la *Loi sur la protection des renseignements personnels et les documents électroniques du Canada* (notifiée sous le numéro de document C(2001) 4539), O.J. L. 002, 04/01/2002 P. 0013-0016.
[151]S.C. 2000, c. 5 [« LPRPDÉ »].

8.5.2 La réponse

Les règles de la LPRPDÉ concernant l'information personnelle essaient d'établir un équilibre entre le droit à la vie privée des personnes et la nécessité pour les organisations de recueillir, d'utiliser ou de communiquer de l'information personnelle dans un but raisonnable[152]. La Loi a été conçue pour une époque dans laquelle la technologie facilite de plus en plus la circulation et l'échange de l'information.

La LPRPDÉ s'applique maintenant à toutes les organisations non gouvernementales qui recueillent, utilisent ou communiquent de l'information personnelle au cours de leurs activités commerciales (sous réserve de la législation provinciale, comme il est traité ci-dessous). Des « activités commerciales » sont définies comme « toute activité régulière ainsi que tout acte isolé qui revêtent un caractère commercial de par leur nature, y compris la vente, le troc ou la location de listes de donneurs, d'adhésion ou de collecte de fonds »[153]. La LPRPDÉ ne s'appliquera pas aux entreprises provinciales dans les provinces qui ont promulgué des lois qui, de l'avis du gouvernement fédéral, sont essentiellement similaires[154]. Jusqu'à présent, seuls le Québec, l'Alberta et la Colombie-Britannique ont promulgué des lois et, à la date de rédaction du présent document, le gouvernement fédéral n'a pas encore officiellement déclaré que les lois de l'Alberta et de la Colombie-Britannique sont « essentiellement similaires »[155].

La LPRPDÉ (PIPEDA) vise à protéger le *renseignement personnel* qui est « tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresse et numéro de téléphone de son lieu de travail »[156]. Cette définition est assez vaste pour inclure l'information suivante :

- Race
- Origine ethnique
- Couleur
- Âge
- État civil
- Religion
- Éducation
- Dossier médical
- Dossier criminel
- Historique de l'emploi
- Historique financier
- Adresse
- Numéro de téléphone
- Identificateurs numériques comme le Numéro d'assurance sociale
- Empreintes digitales

[152]LPRPDÉ/PIPEDA, s. 3.
[153]LPRPDÉ/PIPEDA, s. s.2(1).
[154]LPRPDÉ/PIPEDA, ss. 30(2), 26(2)(b).
[155]*Loi sur la protection des renseignements personnels dans le secteur privé (An Act Respecting the Protection of Personal Information in the Private Sector),* S.Q. 1993, c.17.
[156]LPRPDÉ/PIPEDA, s. 2(1).

- Groupe sanguin
- Échantillon biologique ou de tissu
- Points de vue ou opinions personnelles

Les restrictions imposées en matière de collecte, d'utilisation et de divulgation des renseignements personnels en vertu de la LPRPDÉ se trouvent à l'annexe 1 de la Loi (Annexe). L'Annexe est en fait une déclaration non modifiée du *Code type sur la protection des renseignements personnels* (Code type)[157] de l'Association canadienne de normalisation. Le Code type comprend les dix principes de responsabilité en matière de renseignements personnels. Ces principes contiennent à leur tour des obligations importantes. En vertu de l'article s.5(1), chaque organisation régie par la LPRPDÉ doit se conformer aux obligations établies dans l'Annexe.

La LPRPDÉ établit une série de principes en matière de responsabilité auxquels doivent adhérer ceux qui recueillent les renseignements personnels. Au cœur de ces principes se trouve le concept du consentement informé. Les principes visent à s'assurer qu'une personne doit savoir à quelles fins les renseignements personnels sont recueillis et elle doit pouvoir consentir à de telles fins. En outre, selon ces principes, les renseignements personnels ne doivent pas servir à des fins auxquelles la personne n'a pas consenti.

L'examen détaillé de ces principes de fond est au-delà de la portée du présent document[158]. Nous voulons plutôt attirer l'attention sur le mécanisme de responsabilité qui se trouve dans l'Annexe. Le premier principe énoncé dans l'Annexe (dont tous les principes servent le principe de responsabilité) est le plus important pour nos besoins puisqu'il est intitulé « Responsabilité ». Il déclare ce qui suit : « Une organisation est responsable des renseignements personnels dont elle a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des [principes énoncés dans l'Annexe]. » Même si ces personnes identifiées peuvent déléguer quelques-unes de leurs tâches, elles ont l'ultime responsabilité du traitement des renseignements personnels dans leur organisation. En outre, l'identité de ces personnes doit être communiquée sur demande.

Les personnes désignées ont également la responsabilité d'établir des procédures pour protéger les renseignements personnels qui sont sous la garde de leur organisation. Elles doivent également établir des procédures pour recevoir les plaintes et les demandes de renseignements et y donner suite, pour assurer la formation du personnel et la transmission au personnel de l'information relative aux politiques et pratiques de l'organisation et pour rédiger les documents explicatifs concernant ces politiques et procédures.

Si une personne a une plainte au sujet des pratiques de l'organisation en matière de renseignements personnels, elle doit tout d'abord communiquer avec les personnes désignées. Si elle n'obtient pas des résultats satisfaisants, la personne peut déposer une plainte auprès du Commissaire à la protection de la vie privée qui a le pouvoir de mener une vérification des

[157]CAN/CSA-Q830-96 (Etobicoke, Ontario : Association canadienne de normalisation, 1996).
[158]Pour une explication détaillée de la LPRPDÉ (PIPEDA) et de l'historique de la Loi, voir C.H.H. *McNairn and A.K. Scott, A Guide to the Personal Information Protection and Electronic Documents Act*, 2004 Edition, (Markham, Ontario: LexisNexis Canada Inc., 2003).

pratiques de l'organisation en matière de vie privée. Le Commissaire publiera un rapport avec ses résultats et recommandations, le cas échéant. Si la personne est toujours insatisfaite, elle peut demander une audience à la Cour fédérale.

8.5.3 Les résultats

Étant donné que la LPRPDÉ (PIPEDA) n'a été entièrement mise en œuvre que pendant une brève période de temps, son efficacité en tant que mécanisme de responsabilité reste encore à prouver. Il y a ceux qui croient, comme le professeur Richard Owens de l'Université de Toronto, que la LPRPDÉ fera très peu pour assurer la protection de la vie privée et qu'elle crée en même temps un environnement d'incertitude pour les affaires. Il estime que la LPRPDÉ contient des « incohérences et des erreurs » qui la rendent « terriblement difficile à interpréter même pour un avocat spécialisé »[159]. Toutefois, le réputé professeur de l'Université d'Ottawa, Michael Geist, spécialiste du droit cybernétique, estime que la LPRPDÉ impose « une norme nationale de protection de la vie privée qui offre aux entreprises une plus grande certitude et aux particuliers des protections minimales garanties »[160]. Il sera impossible de déterminer laquelle de ces opinions, le cas échéant, est la bonne jusqu'à ce que nous ayons la possibilité d'examiner l'application de la LPRPDÉ avec le temps.

8.6 La Loi sur la transférabilité et la responsabilité en matière d'assurance-santé aux États-Unis (HIPAA)

8.6.1 Le problème

Les soins de santé aux États-Unis sont fournis au moyen d'un système qui combine des programmes gouvernementaux et de l'entreprise privée. Les nombreuses et diverses entités qui participent à ce système utilisent de plus en plus les moyens électroniques pour partager l'information au sujet des patients lorsque des services médicaux sont assurés à ces personnes. De tels échanges étaient traditionnellement réglementés par un ensemble de lois d'État. Ce manque de normes juridiques uniformes a laissé des lacunes importantes dans la protection de l'information confidentielle des patients. En 1996, le gouvernement fédéral des États-Unis a adopté des lois qui visaient à assurer une norme nationale de protection de cette information.

8.6.2 La réponse en matière de responsabilité

La loi *Health Insurance Portability and Accountability Act* (HIPAA)[161], essaie, entre autres choses[162], d'assurer la protection de l'information confidentielle sur la santé des patients. Dans la loi HIPAA, cette information confidentielle sur la santé s'appelle Protected Health Information

---

[159]Richard Owens, « Federal privacy law is a dog's breakfast », en ligne : The Toronto Star : <http://www.torontostar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1075677008521&call_pageid=968350072197&col=969048863851>.

[160]Michael Geist, « Canada badly needs a national standard », en ligne : The Toronto Star : <http://www.thestar.ca/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1075677008515&call_pageid=968350072197&col=Columnist1036500183695>.

[161]Droit public (Public Law) 104-191.

[162]Un autre aspect important de la HIPAA, c'est qu'elle protège l'accès à la couverture de santé en limitant les exclusions dans le cas de conditions préexistantes.

(PHI). La teneur de cette protection se trouve en grande partie dans la règle finale de la protection de la vie privée (Règle finale) publiée par le Department of Health and Human Services conformément à la HIPAA[163].

La Règle finale s'applique aux « entités couvertes », ce qui inclut les régimes de santé, les établissements et les fournisseurs des soins de santé[164]. L'examen complet de toutes les obligations imposées aux entités couvertes par la loi est au-delà de la portée de notre présent document. Ce qui suit récapitule les principes de responsabilité concrétisés dans la Règle finale[165].

La Règle finale donne à la personne le droit d'avoir un *avis* adéquat des utilisations et des divulgations de l'information protégée PHI qui peuvent être faites par l'entité couverte ainsi que des droits de la personne et des obligations juridiques de l'entité couverte par rapport à la PHI[166]. La Règle finale établit un certain contenu pour de tels avis.

En général, un fournisseur de soins de santé couvert doit obtenir le consentement de la personne, de la manière prescrite par la Règle finale, avant d'utiliser ou de divulguer la PHI pour exécuter des traitements, des paiements ou des opérations de soins de santé[167]. Si jamais une organisation veut utiliser la PHI dans un but qui n'est pas couvert par le consentement, elle doit obtenir l'autorisation de la personne pour un tel but.

Lorsqu'elle utilise ou divulgue la PHI ou qu'elle demande la PHI d'une autre entité couverte, l'entité couverte doit faire des efforts raisonnables pour limiter l'information de santé protégée au minimum nécessaire aux fins prévues d'utilisation, de divulgation ou de demande[168].

En outre, la Règle finale impose des normes organisationnelles de base qui doivent être mises en œuvre par les entités couvertes, ce qui inclut :

- Des systèmes physiques et organisationnels pour assurer la sûreté et la sécurité de la PHI;
- Un processus selon lequel les politiques internes de protection de la vie privée doivent être créées, mises en œuvre et modifiées;
- Un processus selon lequel les personnes peuvent déposer des plaintes au sujet des pratiques de l'entité en matière d'information de santé protégée (PHI) et
- La désignation d'un agent de la protection de la vie privée chargé d'assurer la conformité de l'entité avec la Règle finale et de veiller à ce que les employés soient bien au courant des pratiques de l'entité en matière de vie privée.

[163]45 C.F.R. pt. 160 [« Final Rule »].
[164]Règle finale (Final Rule), §§ 160.103, 103.
[165]La Règle finale ne renvoie pas aux « principes de responsabilité » *per se*. L'expression est utilisée ici pour désigner les types généraux d'exigences qui se trouvent dans la Règle finale.
[166]Final Rule, § 164.520.
[167]*Ibid*. à § 164.506.
[168]*Ibid*. à § 164.502.

8.6.3 Les résultats

La conformité avec les exigences de fond de la Règle finale s'est révélée un défi pour de nombreuses organisations couvertes par cette règle. Par conséquent, la date limite de conformité a été prolongée. Il faudra donc un certain temps avant que nous puissions mesurer les effets pratiques d'une loi HIPAA entièrement mise en œuvre.

8.7 Leçons en matière de responsabilité dans l'infrastructure d'information essentielle

Les participants dans le secteur ont offert des opinions au sujet des leçons en matière de responsabilité qui étaient associées aux initiatives décrites précédemment. Nous avons fusionné ces opinions avec les nôtres pour proposer des façons selon lesquelles ces leçons *peuvent* s'appliquer à l'infrastructure d'information essentielle. Cela pourrait s'avérer intéressant.

8.7.1 An 2000

Il y a un certain nombre de différences importantes entre le problème An 2000 et le défi d'accroître la fiabilité, l'accessibilité et la sécurité de l'infrastructure d'information essentielle. Les implications de ce qu'il faudrait avoir pour maintenir notre infrastructure d'information essentielle sont sérieuses :

- Nous ne savons pas encore ce qui est requis pour maintenir[169] notre infrastructure d'information essentielle;
- Ce qu'il faut pour maintenir l'infrastructure d'information essentielle changera[170] avec le temps;
- Il n'y a pas de date limite pour l'établissement de mesures de protection de notre infrastructure d'information essentielle;
- Dans de nombreux cas, nous n'avons pas les solutions techniques requises[171] et
- Le maintien d'une infrastructure d'information essentielle au Canada dépendra énormément des étrangers[172].

Notre succès collectif avec l'An 2000 peut être une source de fierté, mais nous devrions résister à la tentation d'assumer que la même approche pourrait réussir à protéger l'infrastructure d'information essentielle du Canada.

---

[169]Ce défi a deux volets. Nous n'avons pas encore identifié les services qui doivent être fournis par notre infrastructure d'information essentielle et nous avons encore à déterminer ce qu'il faut pour maintenir ces services qui sont encore à identifier.

[170]Le problème An 2000 pouvait être décelé dans les programmes informatiques existants. Les services requis par notre infrastructure d'information essentielle changeront avec le temps et la technologie déployée pour offrir ces services évoluera.

[171]Nous ne pouvons même pas nous entendre sur les moyens techniques et sociaux qui devraient être employés pour résoudre le problème du pourriel (Spam ou courriel commercial en masse non sollicité). Et cependant, le pourriel est un irritant clair et immédiat pour tous les utilisateurs de courriel sur Internet.

[172]Notre infrastructure d'information a des connexions et des interdépendances partout dans le monde. Nous n'avons pas d'autre choix que de nous conformer aux normes et conventions établies. Un grand nombre de ces « règles » seront établies par des organismes et dans des groupes sociaux où le Canada n'a qu'un rôle mineur à jouer.

Même si les approches qui ont réussi avec l'An 2000 ne s'appliquent pas particulièrement à l'infrastructure d'information essentielle, l'An 2000 donne un excellent exemple de la façon dont une menace jugée sérieuse peut galvaniser à la fois le secteur public et le secteur privé et donner lieu à des mesures efficaces.

8.7.2 Commission Treadway/Sarbanes-Oxley

La Commission Treadway nous enseigne que la compréhension d'un problème potentiel grave n'est pas suffisante. Même l'identification d'une solution ne donne pas, en soi, de bons résultats. La solution doit être mise en œuvre. Cela exige des ressources et de la volonté, ce qui n'est pas facile à générer en l'absence de catastrophe. Lorsqu'une catastrophe s'est produite sous la forme d'une série de scandales financiers majeurs qui mettaient en cause des compagnies comme Enron et WorldCom, les ressources et la volonté se sont matérialisées rapidement. Sarbanes-Oxley en a été le résultat.

On s'entend généralement pour dire que des catastrophes majeures sont probables dans l'infrastructure d'information essentielle. Si elles ont lieu, le cas échéant, des ressources importantes et la volonté d'accroître la fiabilité de l'infrastructure d'information essentielle peuvent devenir disponibles. Il serait bon pour les personnes qui ont des idées ou de l'intérêt dans des mesures précises visant à accroître la fiabilité de l'infrastructure d'information essentielle de préparer le terrain pour leurs initiatives si jamais des possibilités se présentent à elles. En outre, il serait utile de faire des efforts qui permettent de quantifier et de montrer le potentiel de catastrophe dans l'espoir de stimuler des mesures proactives, comme cela a été fait pour l'An 2000.

8.7.3 Directive de l'Union européenne/LPRPDÉ (PIPEDA)

Des initiatives dans une juridiction peuvent non seulement améliorer les choses dans cette juridiction, mais aussi donner lieu à des initiatives positives correspondantes dans d'autres juridictions. L'infrastructure d'information essentielle du Canada est interconnectée à l'infrastructure d'information mondiale et elle dépend de cette infrastructure. Cela ne signifie pas que le Canada ne peut pas apporter unilatéralement des changements positifs dans sa propre partie de l'infrastructure d'information. Ces changements peuvent se répercuter dans d'autres juridictions, à l'avantage de tous et de chacun.

8.7.4 HIPAA

Bien des gens avancent l'argument que l'économie doit diriger tous les changements importants. La loi HIPAA prouve que cela n'est pas vrai. Des initiatives qui sont coûteuses et impopulaires auprès des corporations peuvent quand même réussir si elles ont assez de soutien de la part de la population. Des changements apportés au cadre de responsabilité dans l'infrastructure d'information essentielle peuvent ajouter plus de coûts que de profits, mais l'expérience de la HIPAA indique que cela n'est peut-être qu'un seul facteur pour décider des mesures à prendre, mais non le facteur décisif.

9.0 Mécanismes courants du régime actuel de responsabilité

Même si l'infrastructure d'information constitue un seul système, on peut la considérer comme ayant cinq types de composants :

1. Produits logiciels
2. Logiciels personnalisés
3. Systèmes
4. Services des technologies de l'information (TI)
5. Matériel

Dans cette section, nous présentons les mécanismes de responsabilité qui s'appliquent à cinq types de composants.

9.1 Indemnisation

L'« indemnité » peut être définie comme suit :

> L'indemnité est un type spécifique de mécanisme contractuel d'attribution des risques selon lequel l'une des parties d'un contrat consent à tenir l'autre partie (présumée innocente) exempte de toute réclamation si une tierce partie porte plainte contre la partie innocente[173].

Voici une autre définition : « Une entente selon laquelle une partie consent à protéger l'autre contre une perte ou un dommage prévu[174]. »

L'indemnisation peut servir à décrire diverses obligations légales. Même si une indemnité peut être comparée à une police d'assurance contractuelle, cette description n'est pas techniquement exacte d'un point de vue pratique ou juridique. L'indemnisation a essentiellement trait à la gestion des risques. Certaines indemnités sont fondées sur la description mentionnée ci-dessus de la « partie innocente » alors que d'autres sont basées sur un événement. En ce qui concerne le type d'indemnité de la « partie innocente », la personne est poursuivie non pas parce qu'elle a volontairement commis un acte préjudiciable, mais plutôt parce qu'elle a utilisé un produit, donné une licence et payé pour un produit dont la licence aurait dû, d'après l'autre partie, être fournie par cette dernière[175].

L'autre type d'indemnisation, parfois appelé « indemnité d'événement », est plus étroitement lié à une pure attribution des risques. En d'autres termes, si je ne peux pas fournir un service, je m'arrangerai pour que quelqu'un d'autre fournisse ce service et je paierai tous les montants additionnels dus à ma non-performance. De plus, je consens à vous tenir exempt de tous les dédommagements que vous paierez à une autre partie afin d'obtenir le même service. La plupart

---

[173]Joseph Rosenbaum, « Protect Thyself 101: A primer on indemnification », *ZD Net Tech Update*, (18 février 2004), en ligne : ZD Net Tech Update. <http://techupdate.zdnet.com/techupdate/stories/main/indemnification_primer.html>.
[174]*The 'Lectric Law Library Lexicon, s.v.* "indemnity," en ligne : The Lectric Law Library <http://www.lectlaw.com/def/i027.htm>.
[175]Rosenbaum, *supra* note 173.

des clauses d'indemnisation offertes par les donneurs de licence dans leurs accords types entrent dans la catégorie du « fautif innocent ».

Il y a d'autres facteurs dont il faudrait tenir compte avant d'accepter l'offre d'indemnisation des fournisseurs[176] :

1. L'indemnité se limite-t-elle à certains types de réclamations, comme dans la contrefaçon des marques de commerce ou des brevets uniquement? Ou s'étend-elle à la violation du droit d'auteur qui jouit d'une protection à l'échelle mondiale?
2. Y a-t-il des limitations géographiques/territoriales à l'indemnité (par exemple, l'indemnisation se limite-t-elle aux réclamations déposées au Canada uniquement)?
3. La clause d'indemnisation est-elle complète (c'est-à-dire est-ce qu'elle vous défend, vous indemnise et vous tient entièrement exempt de toute perte et de tout dommage, y compris des frais juridiques) ou vous limite-t-elle à un montant fixe d'argent?
4. Est-ce que la clause d'indemnité fixe les dédommagements à ceux qui sont « véritablement et finalement accordés par un tribunal » ou est-ce qu'elle couvre toutes les dépenses auxiliaires associées à ce litige?
5. Si le contrat en question contient une limitation de la clause de responsabilité (une clause qui indique que, peu importe ce qui se produit, le maximum versé sera de « X » dollars), est-ce que cette limite plafonne votre indemnisation?
6. Si une réclamation est couverte par l'assurance, est-ce que cette couverture chevauche la clause d'indemnisation ou entre-t-elle en conflit avec cette clause?

Les questions ci-dessus montrent bien que le sujet de l'indemnisation est assez complexe. Idéalement, les dispositions en matière d'indemnisation devraient être personnalisées selon le cas à l'étude.

Dans les entreprises qui appuient l'infrastructure d'information essentielle, l'indemnisation sert à transférer les risques entre les clients et les fournisseurs. Les risques et la responsabilité sont interchangeables aux fins de la présente discussion. Les clauses d'indemnisation se trouvent dans les licences ou dans les contrats des produits logiciels, des logiciels personnalisés, des systèmes et des services TI.

Un exemple très connu aujourd'hui d'indemnisation dans le domaine du logiciel est celui de la réponse du groupe Linux aux allégations de SCO selon lesquelles Linux viole certains droits d'auteur détenus par la SCO dans le cas du système d'exploitation UNIX. Afin de calmer les préoccupations des clients au sujet des responsabilités éventuelles, y compris les coûts de la défense en droit, plusieurs fournisseurs Linux, seuls ou de concert, sont en train d'offrir proactivement d'indemniser des clients pour ces coûts. Même si les clauses d'indemnisation ont fait les manchettes dans les journaux récemment à cause des différends Linux/SCO,

[176] *Ibid*.

l'indemnisation a rempli une fonction dans presque tous les contrats sur les technologies et les TI pendant de nombreuses années[177].

À titre d'exemple, une clause d'indemnisation (de RealNetworks Inc., pour son logiciel RealOne Player) est reproduite ici[178] :

> 11. INDEMNISATION. Ce logiciel et les services ne doivent être utilisés qu'avec les médias, le contenu et les outils de création de contenu qui ont la licence appropriée. Vous avez la responsabilité de vérifier si des droits d'auteur, des brevets ou d'autres licences sont nécessaires et d'obtenir ces licences pour servir et/ou créer, comprimer ou télécharger de tels médias et contenus. Vous consentez à n'enregistrer, à ne lire et à ne télécharger que les documents pour lesquels vous avez le brevet, le droit d'auteur et autres permissions, licences et/ou autorisations nécessaires. Vous acceptez de dégager de toute responsabilité, d'indemniser et de défendre RN [RealNetworks], ses agents, administrateurs et employés contre les pertes, dommages, amendes et dépenses (y compris les honoraires et frais des avocats) dus ou liés à des réclamations selon lesquelles vous avez (i) visualisé, téléchargé, codé, comprimé, copié ou transmis des documents (autres que ceux fournis par RN) en rapport avec le logiciel, et ce, en violation des droits d'une autre partie ou en violation d'une loi ou (ii) en violation des modalités du présent contrat de licence. Si vous importez le logiciel des États-Unis, vous devez indemniser RN et tenir la compagnie RN exempte des droits d'importation et d'exportation ou d'autres réclamations dues à cette importation.

9.2 Droit de la responsabilité délictuelle

9.2.1 Introduction au droit de la responsabilité délictuelle ou « Tort Law »

« Tort » est dérivé du latin *tortus*, qui signifie déformé ou tordu. Le terme a été introduit dans l'ancien anglais comme synonyme de « faute »[179]. En français, le mot « tort » signifie également « faute ». Le droit de la responsabilité délictuelle renvoie à cette facette de la loi qui permet à une personne lésée d'obtenir compensation de la personne qui a causé le préjudice[180].

Un délit civil (« tort ») est un acte fautif (autre qu'une violation de contrat) pour lequel on peut obtenir réparation sous forme de dommages-intérêts ou d'injonction. Le droit de la responsabilité délictuelle a pour fonction de décourager une conduite fautive et d'indemniser ceux qui ont subi des préjudices à la suite d'une telle conduite[181]. Alors que le droit contractuel se fonde énormément sur les obligations imposées par des échanges ou des négociations, le droit de la responsabilité délictuelle découle du devoir de diligence imposé par la loi. Peut-être que la

---

[177] *Ibid*.
[178] RealNetworks Inc. *End User License Agreement* (2004), en ligne : Network Computing News <http://www.ncns.com/RealNetworksLicense.html>.
[179] Allen M. Linden, *Canadian Tort Law*, 5th ed. (Toronto: Butterworths, 1993) à 1. (La quatrième édition a été traduite sous le titre de La responsabilité civile délictuelle.)
[180] Lloyd Duhaime, « Tort Law in Canada-An Introduction », *Duhaime's Law Dictionary*, (2004), en ligne : Tort & Personal Injury <http://www.duhaime.org/Tort/ca-negl.htm#general>[Duhaime « Tort Introduction »].
[181] Cynthia A. Patterson & Stewart D. Personick, eds., *Critical Information Infrastructure Protection and the Law*, (Washington, D.C.: The National Academies Press, 2003) à 45, en ligne : The National Academies Press <http://books.nap.edu/catalog/10685.html>[Patterson & Personick, Critical Information Infrastructure Protection and the Law].

meilleure définition globale du droit de la responsabilité délictuelle offerte à ce jour est la suivante : « Un délit est une faute civile, autre qu'une violation de contrat, que la loi redressera par un octroi de dommages-intérêts[182]. »

Chaque personne est censée se conduire d'une manière qui ne porte pas préjudice aux autres. Lorsque quelqu'un porte préjudice à d'autres, que ce soit délibérément ou par négligence, le tribunal peut lui demander de verser de l'argent à la partie lésée (dommages-intérêts) pour qu'en dernier ressort il soit responsable du préjudice causé par l'acte délictueux. L'indemnisation joue probablement le rôle social le plus important dans la responsabilité civile délictuelle[183].

9.2.2 Négligence

Le droit de la négligence est un élément important du droit de la responsabilité délictuelle. Comme il a été énoncé il y a presque 150 ans dans une cause en Angleterre :

> La négligence est l'omission d'une action qu'un homme raisonnable, guidé par les considérations qui règlent généralement la conduite des affaires humaines, ferait; la négligence est aussi de faire une action qu'un homme prudent et raisonnable ne ferait pas. Les défendeurs pourraient avoir été coupables de négligence si, involontairement, ils ont omis de faire ce qu'une personne raisonnable aurait fait ou s'ils ont fait ce qu'une personne prenant des précautions raisonnables n'aurait pas fait[184].

Le principe fondamental du droit de la négligence est connu sous le nom de « principe du prochain ». Ce principe a été adopté en premier par Lord Atkin dans la décision fondamentale au Royaume-Uni de *Donoghue* c. *Stevenson*[185] afin de souligner une « conception générale des relations qui donne lieu à l'obligation de diligence dont les cas particuliers qui se trouvent dans les livres ne sont que des instances ».

Lord Atkin a déclaré :

> « En droit, l'équivalent de la règle voulant que l'on aime son prochain est qu'il ne faut pas causer de préjudice à celui-ci. Et la question que se pose l'avocat de savoir qui est le prochain reçoit une réponse restrictive. Il faut exercer une prudence raisonnable pour éviter les actions ou les omissions qui, selon ce que nous pouvons raisonnablement prévoir, sont susceptibles de causer un dommage à notre prochain. À la question de savoir qui donc, au regard de la loi, est mon prochain, il semble que la réponse soit celle-ci : les personnes que mon acte touche si directement que je devrais raisonnablement envisager que l'action ou l'omission considérée est susceptible de les toucher ainsi[186]. »

Cette idée a servi de guide pour les décisions ultérieures des tribunaux où l'on a déclaré qu'il y a généralement une obligation à remplir chaque fois qu'un préjudice est raisonnablement prévisible à moins que des raisons valides de politique ne réfutent une telle obligation.

---

[182]Linden, *supra* note 179 à 1-2.
[183]Duhaime « Tort Introduction », *supra* note 179.
[184]*Blyth v. Birmingham Water Works* (1856), 11 Ex. 781.
[185]*Donoghue v. Stevenson* [1932] A.C. 562 (H.L.).
[186]*Ibid*. à 580. (La citation en français est tirée d'une fiche de Termium.)

La Cour suprême du Canada a raffiné le test de l'obligation avec une approche à deux étapes dans l'affaire *Kamloops* c. *Nielsen*[187] où la Cour a séparé le test en deux volets :

> (1) Y a-t-il des relations suffisamment étroites entre les parties ... pour que les autorités aient pu raisonnablement prévoir que leur manque de diligence pourrait causer des dommages à la personne en cause? Dans l'affirmative,
>
> (2) Existe-t-il des motifs de restreindre ou de rejeter
>
> (a) la portée de l'obligation et
> (b) la catégorie de personnes qui en bénéficient ou
> (c) les dommages auxquels un manquement à l'obligation peut donner lieu?

Cette approche à deux étapes a été uniformément suivie dans d'autres décisions de la Cour suprême du Canada[188].

Le droit de la négligence déclare qu'une personne qui cause un préjudice (le défendeur) à une autre personne (le demandeur) par manquement à la norme raisonnable de prudence sera responsable envers le demandeur des préjudices causés au demandeur, en supposant qu'il est déterminé que le défendeur devait au demandeur une obligation de diligence. En général, afin d'obtenir des dommages-intérêts pour les torts qui lui ont été causés, le plaignant doit démontrer que le défendeur était négligent.

9.2.3 Critères d'établissement de la négligence

Afin d'établir une cause d'action pour négligence, plusieurs éléments doivent être présents[189]. Dans son texte *Canadian Tort Law* (La responsabilité civile délictuelle), le juge Allen M. Linden mentionne six critères qui doivent être présents pour établir une cause d'action pour négligence :

1. Le demandeur doit avoir subi un préjudice;
2. Le préjudice subi doit être causé par la conduite du défendeur;

---

[187][1984] 2 S.C.R. 2, à 10.

[188]Ces décisions incluent *B.D.C. Ltd.* v. *Hofstrand Farms Ltd*., [1986] 1 S.C.R. 228, at p. 243 (per Estey J.); *Just* v. *British Columbia* (1989), 64 D.L.R. (4th) 689 (S.C.C.); *Rothfield* v. *Manolakos* (1989), 63 D.L.R. (4th) 449 (S.C.C.) (per Cory J.), etc.

[189]Il y a un minimum de désaccord quant au nombre réel des éléments requis. L'approche traditionnelle britannique envers la responsabilité pour négligence, aussi connue sous le nom de « règle A.B.C. », exige que le demandeur établisse trois éléments dans le cadre d'une action pour négligence à la satisfaction du tribunal : (a) une obligation de diligence existe; (b) il y a eu violation de cette obligation et (c) cette violation a causé un préjudice. Toutefois, cette approche simple ne règle pas suffisamment la question de l'étendue de la responsabilité.

Des spécialistes américains [*Prosser and Keeton on the Law of Torts,* 5th ed. (1984)] ont suggéré que quatre éléments sont nécessaires pour établir une cause d'action pour négligence :
(a) une obligation; (b) un manquement à la norme requise; (c) un lien causal raisonnablement étroit entre la conduite et le préjudice subi (parfois appelé « cause immédiate ») et (d) un préjudice réel ou une perte ayant pour résultat l'intérêt d'une autre personne. Toutefois, ce schème peut également entraîner des difficultés. Un tribunal peut parfois interpréter la question de la cause immédiate en fonction de l'obligation ou de l'éloignement, ce qui a pour résultat de fusionner le premier et le troisième éléments. En outre, les tribunaux confondent parfois l'obligation avec le manquement à la norme requise. De plus, cette approche ne tient pas compte de la conduite du demandeur comme élément à envisager dans l'établissement de la cause d'action.

3. La conduite du défendeur doit être négligente (c'est-à-dire en violation de la norme de prudence établie par la loi);
4. Il doit y avoir une obligation reconnue par la loi pour éviter ce préjudice;
5. La conduite du défendeur doit être une cause immédiate de la perte (en d'autres termes, le préjudice ne devrait pas être un résultat trop éloigné de la conduite du défendeur) et
6. La conduite du demandeur ne devrait pas faire obstacle à l'obtention de dommages-intérêts, c'est-à-dire que le demandeur ne doit pas être coupable de négligence concourante et il ne doit pas assumer volontairement le risque[190].

En général, avant que la responsabilité pour négligence puisse être établie, le demandeur doit fournir la preuve de tous les éléments nécessaires à l'appui de sa réclamation[191].

Les tribunaux déterminent généralement ce qu'est la norme raisonnable de prudence dans une situation donnée. Si cette norme n'est pas respectée, le tribunal doit alors décider qui a droit à l'indemnité à cause du manquement à la norme du défendeur. L'un des principaux buts du droit de la négligence est d'encourager un comportement plus prudent grâce à l'adoption de mesures effectives afin d'éviter des scénarios qui donnent lieu à des préjudices.

9.2.4 Droit de la responsabilité civile et infrastructure d'information essentielle

Le fonctionnement de l'infrastructure d'information peut donner lieu à un certain nombre de questions dans la sphère du droit de la négligence. Il y a des questions qui ont trait à la négligence dans le domaine de la fabrication des ordinateurs et des produits d'information, particulièrement à la lumière des cycles toujours plus courts des produits. D'autres questions liées à la négligence peuvent être dues au fait que le logiciel exempt d'erreurs reste un but inatteignable (au moins dans l'avenir prévisible)[192]. En outre, l'utilisation elle-même des ordinateurs et des produits d'information peut entraîner de la négligence.

En réalité, on a signalé peu de cas de réclamations dues à la négligence contre les fabricants et les développeurs des éléments de l'infrastructure d'information essentielle, comme les ordinateurs, les logiciels et autres produits liés à l'information. L'une des raisons en est que, dans la plupart des cas, les préjudices causés par le mauvais fonctionnement de ces produits se limitaient surtout à des pertes économiques plutôt qu'à des blessures aux personnes ou à des dégâts à la propriété. Par conséquent, la plupart des réclamations contre les fournisseurs ont été faites dans le domaine des contrats (volet du droit qui se prête mieux à l'indemnisation de perte économique pure)[193].

Un autre facteur qui rend difficile l'application des principes de négligence à l'infrastructure d'information essentielle est celui de déterminer quelle norme de prudence il faut appliquer au développement d'un système informatique ou d'un programme logiciel. Tout d'abord, il n'y a pas d'exigences uniformes de licence ou de certification dans le cas des ingénieurs ou des

[190]Linden, *supra* note 179 à 93.
[191]Patterson & Personick, *supra* note 181 à 45-46.
[192]George S. Takach, *Computer Law*, 2d ed. (Toronto: Irwin Law, 2003) à 457.
[193]*Ibid*. à 459.

développeurs de logiciels. En second lieu, il n'y a pas de normes générales en place pour la programmation, la conception ou les tests des logiciels (par exemple, il n'y a rien d'analogue au Manuel de l'ICCA qui est utilisé dans la profession comptable). Par conséquent, il n'y a pas de normes généralement acceptées parmi les professionnels des logiciels quant au nombre de tests qu'un nouveau produit devrait subir ou au nombre d'erreurs qu'il peut y avoir par ligne de codes avant qu'un produit puisse être distribué sur le marché[194].

En ce qui concerne les attaques délibérées contre l'infrastructure d'information essentielle, comme les attaques par déni de service, il est évident que le pirate qui a causé le préjudice devrait en avoir la responsabilité délictuelle. Toutefois, la question la plus difficile est celle de savoir si la responsabilité en cas de négligence devrait également s'appliquer aux entités (compagnies, fournisseurs, fournisseurs de service, universités, particuliers et ainsi de suite) dont les systèmes ou les produits ont été utilisés dans l'attaque et qui ont négligé de prendre des mesures raisonnables pour se protéger contre une mauvaise utilisation de leurs réseaux avant l'attaque[195]. Il n'y a pas eu de cas de ce type au Canada et, jusqu'à ce jour, aucun tribunal américain n'a abordé la question de la responsabilité par manque de protection adéquate d'un réseau informatique. On peut penser que, si le droit de la responsabilité civile s'applique aux questions de la sécurité informatique de l'infrastructure d'information essentielle, le risque de poursuites avec les dommages-intérêts correspondants pourrait stimuler l'investissement dans de plus grandes mesures de sécurité de l'infrastructure d'information.

Une autre zone d'incertitude quant à l'applicabilité du droit de la responsabilité délictuelle est celle de savoir s'il faut recouvrer les dommages-intérêts auprès d'une compagnie dont les réseaux ont été mal sécurisés et ont été utilisés ensuite par un tiers pour causer des préjudices. Comme il a été mentionné précédemment, pour recouvrer des dommages-intérêts en vertu du droit de la responsabilité délictuelle, le demandeur doit démontrer que le défendeur a été négligent. Toutefois, étant donné les éléments mentionnés ci-dessus qui sont nécessaires à l'établissement d'une cause d'action pour négligence, le demandeur aurait de la difficulté à satisfaire à toutes les exigences du scénario factuel sur la sécurité de réseau mentionné ci-dessus. En effet, il n'y a actuellement aucune obligation juridique entre un fournisseur de service et d'autres parties non liées (ou « en aval ») sur l'Internet. S'il devait y avoir une telle obligation à l'avenir, elle devrait se fonder sur la décision dans l'intérêt public que les victimes doivent avoir un recours légal, que le risque de préjudice était prévisible, que le défendeur pouvait en partie amoindrir ou contrôler le risque de préjudice et que le défendeur était la partie qui était le plus en mesure d'assurer la protection contre ce préjudice[196].

Il y a eu des cas aux États-Unis[197] où l'on a considéré la question de la prévisibilité du préjudice à des tiers dans le contexte des réseaux informatiques. Dans ces cas, il fallait décider si oui ou non le défendeur *savait ou aurait dû savoir* qu'une conduite préjudiciable avait lieu dans ses

---

[194]*Ibid*.
[195]Patterson & Personick, *supra* note 181 à 45.
[196]*Ibid*. à 46.
[197]*Cubby* v. *CompuServe*, 776 F. Supp. 135 (S.D.N.Y. 1991); *Stratton Oakmont* v. *Prodigy*, 1995 WL 323710 (N.Y.Sup.Ct.); *RTC* v. *Netcom* , 907 F. Supp. 1361 (N.D.Cal. 11/21/95); *A&M Records, Inc*. v. *Napster, Inc*., 239 F.3d 1004 (9th Cir. 2001); *Cyber Promotions* v. *Apex Global Information Services*, 61997 WL 634384 (E.D. Pa. 1997).

réseaux (par opposition à « probablement aura lieu »). Même si les décisions dans ces cas ont été prises dans des contextes différents, essentiellement la violation du droit d'auteur et le droit de la diffamation, les principes juridiques sont transférables et applicables. Les décisions laissent croire que le fait de tenir les défendeurs responsables des préjudices causés par des vulnérabilités connues de la sécurité des réseaux, mais non réglées, serait un prolongement rationnel et logique de la doctrine légale actuelle. Selon ce raisonnement, si un fournisseur de service sait ou devrait savoir que ses réseaux sont utilisés pour causer des préjudices (et qu'il a la capacité d'empêcher ces préjudices), on peut demander à l'organisation de prendre des mesures pour prévenir ces préjudices. Les partisans de l'application de la responsabilité délictuelle à l'infrastructure d'information essentielle déclarent que les organisations qui contrôlent les réseaux informatiques sont les mieux placées pour lancer et appliquer les mesures appropriées de sécurité et qu'elles peuvent mettre ces mesures en œuvre au coût le plus bas.

Le droit de la responsabilité délictuelle pourrait également servir de facteur de motivation et d'accompagnement important lorsqu'il s'agit d'établir des normes et des pratiques exemplaires à l'échelle de l'industrie puisque la conformité avec ces normes démontre généralement que l'on a rempli l'obligation de prudence et de diligence[198]. Si la responsabilité pour négligence devait être reconnue comme applicable dans ce domaine, l'organisation pourrait alors minimiser sa responsabilité grâce à la mise en œuvre de normes de sécurité. Pour l'instant, toutefois, il n'y a aucune obligation apparente de prudence ni de norme uniformément reconnue de diligence dans le domaine de la sécurité des ordinateurs/des réseaux. En outre, la sélection d'une telle norme serait très complexe à cause de la nature évolutive des vulnérabilités en matière de sécurité ainsi que de l'énorme diversité des entités qui constituent l'infrastructure d'information essentielle.

Par exemple, une norme de « diligence raisonnable » pourrait inclure la pratique d'installer et d'appliquer rapidement des correctifs de sécurité. Toutefois, il serait difficile de décider de la fréquence à laquelle ces correctifs pourraient être appliqués afin de respecter une telle norme. En outre, même si un correctif peut régler une vulnérabilité dans un système, il pourrait donner lieu à une nouvelle vulnérabilité. Au regard du droit de la responsabilité délictuelle, une organisation qui installe un correctif qui laisse son système plus vulnérable devrait-elle être jugée négligente? En outre, les correctifs entraînent parfois d'autres erreurs dans le système en créant d'autres vulnérabilités. Ne serait-ce pas plus prudent des fois de retarder l'installation d'un correctif jusqu'à ce que l'on puisse montrer qu'il est « sûr »?

Une autre question restée sans réponse est celle de savoir si toutes les entités dans l'infrastructure d'information essentielle devraient suivre la même norme de diligence et de prudence en ce qui concerne la sécurité des réseaux informatiques. Dans le droit de la responsabilité délictuelle, on détermine souvent la responsabilité pour négligence en désignant les parties qui sont le mieux placées pour empêcher les événements préjudiciables. Dans le cas des attaques distribuées de déni de service, les fournisseurs de service Internet occupent une place privilégiée pour ce qui est d'empêcher ou d'atténuer les préjudices dus à des attaques de déni de service. En effet, ces fournisseurs peuvent localiser certaines attaques de réseau lorsque ces attaques pénètrent leurs systèmes. Même si les fournisseurs de service Internet pouvaient prévenir et intercepter les attaques, ils ont actuellement peu d'encouragements à cet effet. La mise en œuvre de meilleurs

[198]Patterson & Personick, *supra* note 181 à 51.

protocoles de sécurité de réseau augmenterait les dépenses et pourrait détériorer les performances globales du réseau, entraînant ainsi le mécontentement des clients. Par ailleurs, les attaques de déni de service ont aussi pour résultat des clients mécontents. Comme les fournisseurs de service Internet sont en grande partie déréglementés, il n'y a pas de normes officielles de sécurité ou de fiabilité du service auxquelles ils doivent adhérer. Ainsi, leurs réactions aux incidents comme les attaques de réseau sont variables et dépendent beaucoup de leur propre bon vouloir et des forces concurrentielles du marché[199].

Quelques commentateurs juridiques ont soutenu que les fournisseurs de service Internet devraient assumer une grande responsabilité pour négligence dans le cas de systèmes et de réseaux non sécurisés puisque ces fournisseurs savent (ou devraient savoir) quels sont les risques inhérents et qu'ils ont la capacité de diminuer ou d'arrêter les attaques de déni de service. Par ailleurs, certains fournisseurs de service Internet soutiennent qu'ils devraient être dégagés de toute responsabilité pour le trafic malveillant qui passe par leurs réseaux car ils sont tout simplement des porteurs de signaux courants.

9.3 Droit pénal

Le droit pénal est l'un des mécanismes les plus clairs d'attribution et d'application de la responsabilité. La véritable nature et la quantité des crimes informatiques ne sont pas délimitées avec précision. Quant au niveau de ces crimes, des statistiques précises et fiables sont difficiles à obtenir. Il y a deux raisons à cela. Tout d'abord, une certaine proportion des activités criminelles dans le domaine informatique est difficile à détecter. En second lieu, de nombreuses victimes, même lorsqu'elles se rendent compte du crime, ont de la réticence à le signaler à cause des impacts négatifs éventuels sur leur réputation auprès des clients et des investisseurs. Toutefois, c'est un fait bien établi que les crimes informatiques représentent un problème important et en croissance.

L'une des définitions de crime informatique est celle « d'un comportement illégal, contraire à l'éthique ou non autorisé qui porte sur le traitement automatique des données et/ou sur la transmission des données »[200]. Une autre définition de crime informatique, utilisée par la GRC, est qu'il s'agit « d'un acte illégal qui touche un système informatique, que l'ordinateur soit l'objet du crime, un instrument qui a servi à commettre le crime ou un dépôt de preuves liées à un crime »[201]. D'après ces définitions (et de bien d'autres), on peut voir que le crime informatique couvre un domaine très vaste.

Dans l'optique du droit pénal (qui touche aux mécanismes actuels de responsabilité), nous avons identifié trois acteurs importants :

1. Les législateurs
2. Les exécuteurs
3. Les criminels

---

[199] *Ibid*. à 53.
[200] Ulrich Sieber, *The International Emergence of Criminal Information Law* (Koln: Heymanns, 1994) à 5, cité dans Takach, *supra* note 192 à 209.
[201] Takach, *supra* note 192 à 209.

Chaque groupe sera traité dans le contexte de la responsabilité.

9.3.1 Les législateurs

Le droit pénal au Canada relève essentiellement du *Code criminel* du Canada. En substance, le *Code criminel* définit le comportement que la société, par l'entremise du Parlement, a jugé être socialement inacceptable[202]. Les articles du *Code criminel* qui sont les plus pertinents dans la mise en accusation et la poursuite de personnes qui utilisent la technologie informatique pour des gains non autorisés, pour la destruction, la manipulation, l'intrusion ou pour toute tentative de distribution d'images ou de discours socialement inacceptables portent sur ce qui suit : vol, fraude, utilisation frauduleuse d'un ordinateur, utilisation frauduleuse des données, obscénité/pornographie juvénile, propagande haineuse et interception des communications. En outre, selon la nature du crime et l'étendue du rôle joué par l'infrastructure d'information dans la perpétration d'une infraction, d'autres cas d'infractions dans le *Code criminel* peuvent s'appliquer de temps en temps.

Il est utile de noter qu'en général le droit criminel a toujours porté sur la protection des biens tangibles et sur la sécurité des particuliers. Toutefois, comme l'infrastructure d'information est caractérisée par des changements technologiques rapides, combinés aux qualités éphémères et insaisissables de l'information, les législateurs ont relevé un important défi en mettant à jour et en révisant le *Code criminel* de manière à pouvoir traiter avec efficacité les nouveaux méfaits possibles dus à l'utilisation des ordinateurs et des réseaux[203]. Plusieurs modifications apportées au *Code criminel* dans les dernières années ont des dispositions sur les ordinateurs. Toutefois, l'utilisation accrue des ordinateurs et de l'Internet, ainsi que la plus grande dépendance envers l'infrastructure d'information, a soulevé et continuera probablement de soulever des questions difficiles et de présenter des défis à la fois en vertu des nouvelles clauses et des clauses plus anciennes du *Code criminel*. Pour assurer un niveau adéquat de responsabilité, les législateurs devront sans doute revoir les articles pertinents du *Code criminel* afin de suivre le rythme des changements technologiques.

Nous devrions également noter que les législateurs peuvent être fortement influencés par les pressions politiques. En outre, quelles que soient les nouvelles lois adoptées pour l'infrastructure d'information, les juges sont libres d'appliquer et d'interpréter ces lois au cas par cas, selon les faits de chaque cas individuel et les décisions des tribunaux dans d'autres juridictions[204].

9.3.2 Les exécuteurs

Dans le programme total de répression de tous les crimes, l'importance des crimes cybernétiques dépend du type et de la gravité de la véritable infraction criminelle à l'étude. Dans de nombreuses infractions de ce genre, particulièrement celles qui portent sur l'utilisation de l'Internet, l'un des facteurs importants est celui de la disponibilité des ressources pour bien mener l'enquête. En outre, la quantité de ressources consacrées à la répression d'un type

[202]Voir Kent Roach, *Criminal Law* (Toronto: Irwin Law, 1996), à 2 : « Le droit criminel est essentiellement conçu pour dénoncer et pour punir un comportement intrinsèquement fautif et pour dissuader les gens de commettre de crimes ou d'adopter un comportement qui présente un risque de préjudice grave. »
[203]Takach, *supra* note 192 à 228.
[204]Entrevue de Keith L. Geurts, Associate, Gowlings Lafleur Henderson (26 février 2004) [Geurts interview].

particulier d'infractions cybernétiques tend à être proportionnelle à la perception qu'a la société de l'importance de prévenir cette infraction en particulier[205].

Par exemple, la protection des enfants a été jugée par nos tribunaux et par le gouvernement comme un facteur prépondérant dans l'attribution des fonds et des services pour prévenir les activités criminelles contre les enfants. La pornographie juvénile, par exemple, peut maintenant être facilement transmise dans le monde entier par l'Internet. Cette accessibilité a eu un impact sur la quantité des ressources attribuées à la lutte contre ces crimes. Il n'est donc pas inhabituel, pour les services de police, d'établir des groupes de travail afin de surveiller les cas de possession et de distribution de la pornographie juvénile sur l'Internet et d'enquêter à ce sujet et aussi de travailler main dans la main avec d'autres juridictions au Canada et à l'échelle internationale pour combattre ce genre de crime.

À cause de ressources limitées, nos services de police comptent également sur le public et sur le milieu des affaires pour les aider à combattre les crimes cybernétiques. La lutte contre la fraude des cartes de crédit, par exemple, est un effort conjoint entre les compagnies de cartes de crédit, la communauté et les services de police. En haut de cette chaîne, on trouve les services de vérification internes des compagnies de cartes de crédit qui détectent et surveillent toute activité frauduleuse. Réciproquement, lorsque les services de police sont au courant d'escroqueries dans ce domaine, ils communiquent avec les compagnies et avec les propriétaires des cartes de crédit. Finalement, tous les détenteurs de cartes de crédit ont l'obligation de surveiller l'activité de leurs propres cartes de crédit et de signaler toute activité frauduleuse dès qu'ils sont au courant.

En vertu du *Code criminel*[206], des peines minimales doivent être imposées pour certaines infractions. Pour ces infractions, comme le fait de conduire avec des facultés affaiblies, la société a imposé une condition obligatoire selon laquelle la personne condamnée pour la première fois aura un casier judiciaire, une suspension du permis de conduire et une amende. Le juge qui préside ne peut pas imposer une peine inférieure. Toutefois, il n'y a pas de peines minimales pour ce qui est de la fraude. Comme pour tous les crimes qui n'exigent pas de peine minimale, il existe beaucoup de variations entre les peines imposées pour les fraudes par les différents juges et les différentes juridictions. Cela peut mener à une attitude générale d'indulgence de la part de certains juges dans le cas des crimes informatiques. Par exemple, en ce qui concerne les infractions de jeunes pirates de scripts appelés « script kiddies », les juges imposeront souvent des sentences extrêmement indulgentes, comme l'absolution conditionnelle ou inconditionnelle, le travail communautaire et ainsi de suite. La justification donnée généralement à l'appui de cette indulgence est que l'accusé n'a pas compris le préjudice que le code malveillant pouvait causer ou encore le juge citera le manque d'une véritable intention malveillante. En outre, le jeune âge de l'auteur de l'infraction et le désir de ne pas imposer à cette personne le stigmate d'un casier judiciaire peuvent représenter des facteurs additionnels en faveur de l'indulgence[207].

[205] *Ibid*.
[206] *Code criminel(Criminal Code),* R.S., c. C-34, s. 1.
[207] Entrevue de Geurts, *supra* note 204.

9.3.3 Les criminels

Il y a plusieurs différences importantes entre les cyber-criminels et les criminels qui ne commettent pas d'infractions liées aux ordinateurs ou à l'infrastructure d'information. Tout d'abord, les cyber-criminels n'ont pas de contact direct avec leurs victimes. Ils commettent en général leur crime à domicile à l'aide d'un écran d'ordinateur[208].

En second lieu, de nombreux cyber-criminels, particulièrement ceux qui sont inexpérimentés ou novices, ne comprennent pas la gravité de leur acte criminel ni même qu'ils peuvent être arrêtés. Le fait que l'acte lui-même soit illégal aura peu d'effet, sinon aucun effet, de dissuasion sur eux. Toutefois, ce qui a vraiment un effet de dissuasion, c'est lorsque des personnes semblables sont arrêtées à cause d'actes de même nature et qu'il y a une grande attention des médias autour de ces personnes.

Un bon exemple en est fourni par les poursuites récentes aux États-Unis contre des personnes qui téléchargeaient illégalement des chansons protégées par droit d'auteur au moyen de services de partage de fichiers de poste à poste. Lorsque les causes de la RIAA (Recording Industry Association of America) étaient en cours, le volume du partage illégal de fichiers et du téléchargement des travaux protégés par droit d'auteur a chuté[209].

Troisièmement, les cyber-criminels plus expérimentés ou « professionnels » comprennent qu'il est possible de dépister les activités criminelles exécutées dans les réseaux informatiques. Par conséquent, ces criminels (qui sont en général très éduqués et sophistiqués sur le plan technologique) prennent de nombreuses précautions qui amoindrissent les risques d'arrestation. En fait, ils estiment, à juste titre, que le risque d'être arrêtés et menés devant la justice est minime[210]. Des lois plus strictes avec des pénalités plus élevées n'auront sans doute pas beaucoup d'effet de dissuasion sur ce groupe.

9.4 Assurance

L'assurance a été un sujet qui est revenu de nombreuses fois au cours des entrevues et dans les publications. Il est clair que les gens s'attendent à ce que l'assurance ait un impact majeur sur la structure de responsabilité de l'infrastructure d'information essentielle. Richard Clarke, ancien président du Critical Information Infrastructure Protection Board aux États-Unis a déclaré : « Le secteur de l'assurance peut jouer un rôle pivot dans la protection du cyberespace en créant des mécanismes de transfert des risques, en travaillant avec le gouvernement pour rendre les entreprises plus conscientes des risques cybernétiques et en collaborant avec les chefs de file de l'industrie technologique pour promouvoir des pratiques exemplaires en matière de sécurité des réseaux[211]. »

---

[208] *Ibid*.
[209] *Ibid*.
[210] *Ibid*.
[211] Information Insurance Institute, News Release, « Most Companies Have Cyber-Risk Gaps in Their Insurance Coverage, States The I.I.I. -- Traditional Insurance Policies Not Adequate For Cyber Exposures », (13 août 2003), en ligne : Insurance Information Institute <http://www.iii.org/media/updates/press.731722/>.

Lorsque nous avons parlé avec des cadres supérieurs dans le domaine de l'assurance, il semblait y avoir des écarts importants entre les perspectives des assureurs, des utilisateurs et des fournisseurs de l'infrastructure d'information essentielle et des experts de l'industrie. Au risque de trop simplifier la situation, nous aimerions offrir les pensées suivantes :

- De nombreux analystes semblent croire que les compagnies d'assurance seront très proactives dans des domaines comme ceux de l'établissement des normes, de la certification des produits et de la certification des utilisateurs.
- Par ailleurs, les compagnies d'assurance semblent enclines à y aller très lentement et avec prudence pour offrir de l'assurance. Cette prudence est justifiée. « Selon certains, les compagnies d'assurance [qui offrent de l'assurance contre les risques cybernétiques] font des choix suicidaires. » « C'est une idée folle », dit Catherine Hajnal, professeur adjoint des Systèmes d'information à l'école de commerce Sprott School of Business de l'Université Carleton[212]. Il est très difficile, sinon impossible, de quantifier beaucoup de ces risques. En outre, les assureurs n'ont pas l'expertise nécessaire pour établir des normes ou des certifications. Ils n'ont pas non plus l'inclinaison ni le stimulant voulu pour développer cette expertise.
- Les utilisateurs ne sont pas assurés en grande partie contre les risques cybernétiques et, de plus, ils ne sont pas au courant de cette lacune dans leur couverture. « Malheureusement, la plupart des compagnies fonctionnent dans un environnement de menaces du 21e siècle avec une couverture d'assurance du 20e siècle, a déclaré John Spagnuolo, cyber-expert de l'Insurance Information Institute (I.I.I.). La dynamique de gestion des risques a changé avec la technologie[213]. »
- Les fournisseurs sont plus sensibles à leurs risques, mais ils subissent une énorme pression économique pour minimiser les primes d'assurance.

Même si la portée du projet ne nous permet pas d'explorer cette question en profondeur, nous nous sentons obligés d'inclure la brève analyse suivante (section 9.4.1). En outre, nous recommandons que d'autres travaux soient entrepris dans le but de favoriser le consensus au sujet de l'évolution de l'assurance dans le domaine de l'infrastructure d'information. Ces travaux s'harmoniseraient avec les forces du marché pour encourager un développement plus rapide et plus souple des produits d'assurance appropriés.

[212]Scott Foster, « Virus victims weigh cyber-insurance options: insurance providers offer policies to cover corporate damage caused by worms such as Blaster » *Computing Canada* (3 octobre 2003), en ligne : looksmart <http://www.findarticles.com/cf_dls/m0CGC/19_29/108992880/p1/article.jhtml>.

[213]John Spagnuolo, cité dans le bulletin Information Insurance Institute, News Release, « Most Companies Have Cyber-Risk Gaps in Their Insurance Coverage, States The I.I.I. -- Traditional Insurance Policies Not Adequate For Cyber Exposures », (13 août 2003), en ligne : Insurance Information Institute <http://www.iii.org/media/updates/press.731722/ >.

9.4.1 Aperçu du marché de l'assurance

L'assurance cybernétique constitue une partie très mineure du secteur total de l'industrie. À cause de cela, l'état actuel et l'évolution de l'assurance cybernétique se comprennent mieux dans le contexte du secteur global de l'assurance. L'excellent aperçu suivant du marché de l'assurance est fourni par Gaston & Associates[214] :

> Les entreprises doivent se préparer pour des changements majeurs dans la disponibilité et les prix de l'assurance. Nous nous attendons à ce que la plupart des compagnies d'assurance, sinon toutes, augmentent les primes pendant l'année qui vient et limitent certaines catégories d'entreprises ou certains types de couvertures. Ces changements ont lieu à l'échelle de l'industrie et ils ne se limitent pas à une compagnie d'assurance en particulier ni à une région géographique particulière.
>
> Même si les événements du 11 septembre ont définitivement eu un effet sur la disponibilité et les prix de l'assurance, des changements avaient eu lieu même avant cet événement. Notre économie était en train de changer et l'industrie de l'assurance avait déjà subi une baisse économique.
>
> Les compagnies d'assurance comptent sur le revenu d'investissement pour faire un profit puisque la prime à elle seule ne suffit pas en général à payer les réclamations. Le revenu d'investissement est utilisé dans le calcul des taux nécessaires au remboursement des réclamations. Vers la fin des années 1980, trop de capital dans l'industrie de l'assurance a eu pour résultat ce que l'on appelle un « marché faible », comme le prouvent les prix hautement concurrentiels des polices d'assurance commerciales. Vers le milieu des années 1990, un rendement exceptionnel dans le marché de l'investissement a créé encore plus de concurrence pour les dollars déboursés en prime entre les compagnies d'assurance, poussant ainsi les primes à des niveaux encore inférieurs. Après 12 ans de conditions de « marché faible », l'industrie a commencé à montrer des signes de tension en 2001 et il semblait y avoir des poches d'activité dans le marché qui signalaient qu'un changement de cycle n'était pas loin. À mesure que le marché de l'investissement commençait à changer, donnant un taux de rendement inférieur aux investisseurs, les compagnies d'assurance commencèrent à augmenter les taux et à être plus sélectives quant aux types de risques qu'elles voulaient couvrir. Cette condition s'appelle un « hard market » ou « marché dur ».
>
> Les compagnies d'assurance achètent également leur propre type d'assurance, appelé réassurance, qui leur permet d'assurer de gros risques et d'étaler le risque sur des comptes plus petits. Les coûts de réassurance pour les compagnies d'assurance étaient déjà en hausse avant le 11 septembre, d'où des primes plus élevées pour les consommateurs. La catastrophe du World Trade Center représente l'événement où il y a eu la plus forte demande de règlements dans l'histoire avec un total estimatif de réclamations dépassant les 40 milliards de dollars. Cet événement a causé une onde de choc dans toute l'industrie de l'assurance, y compris dans le marché de la réassurance, et il a rapidement accéléré ce qui se produisait déjà dans la hausse des prix. Même si on s'attend à ce que toutes les demandes légitimes faites pour le World Trade Center soient réglées par l'industrie de l'assurance, les conséquences financières de cet événement sont énormes.

[214]Gaston & Associates, Inc., « Insurance Market Hardening », en ligne : Gaston & Associates, Inc. <http://www.gastonassoc.com/html/market_hardening.asp>.

> À compter de 2002, les compagnies de réassurance ont nettement augmenté leurs coûts pour les compagnies d'assurance et elles refusent dans certains cas toute couverture pour certains risques, comme le terrorisme. Tout cela retombe finalement sur les clients de la compagnie d'assurance, pour tous les types de couvertures. C'est tout simplement une question d'offre et de demande et, dans ce cas, la demande surpasse l'offre.

9.4.2 L'évolution de la cyber-assurance

Dans la nouvelle édition à paraître de son livre *Secrets and Lies*, l'expert en sécurité cybernétique Bruce Schneier déclare : « Il est évident pour moi que la sécurité informatique n'est pas un problème que la technologie peut résoudre. Les solutions en matière de sécurité ont un élément technologique, mais la sécurité est essentiellement un problème de personnes. Les entreprises abordent la sécurité [et la responsabilité] comme elles le font pour toute autre incertitude dans le domaine des affaires, soit en termes de gestion des risques[215]. »

M. Schneier, avec bien d'autres personnes, croit que les risques seront en hausse pour les entreprises car celles-ci seront de plus en plus tenues responsables de la sécurité (ou du manque de sécurité) de leurs produits et services. Cette responsabilité aura un impact fondamental sur la façon dont les fournisseurs et les utilisateurs se comportent.

« Les propriétaires d'entreprise n'aiment pas l'inconnu, déclare Daniel Egger, président de Open Source Risk Management, si les risques de l'entreprise peuvent être gérés à un coût donné, cette valeur connue peut être intégrée au coût d'exploitation de l'entreprise ou au coût total de possession (CTP/TCO) de la technologie de l'information. Selon la nature du coût, tout (à partir du budget jusqu'au prix des produits ou services) peut refléter les coûts additionnels de gestion des risques[216]. »

L'assurance sera le principal moyen pour les organisations de gérer le coût des risques cybernétiques. Bruce Schneier poursuit :

> Cette [assurance] aura lieu automatiquement car les chefs d'entreprise se tournent vers les compagnies d'assurance pour les aider à gérer les risques et le transfert de responsabilité représente ce que les compagnies d'assurance font. Du point de vue des chefs d'entreprise, l'assurance transforme les risques à coûts variables en dépenses à frais fixes et les chefs d'entreprise aiment les dépenses à frais fixes car elles peuvent être budgétées. Lorsque les chefs d'entreprise commenceront à se soucier de la sécurité – et il faudra appliquer le concept de responsabilité pour qu'ils s'en soucient véritablement – ils vont se tourner vers l'industrie de l'assurance pour demander de l'aide. Les compagnies d'assurance ne sont pas bêtes; elles vont se lancer en grand dans la cyber-assurance et, à ce moment-là, elles vont diriger le secteur de la sécurité informatique… tout comme elles dirigent le secteur de la sécurité dans le monde des biens tangibles[217].

---

[215]Bruce Schneier, *Secrets and Lies, Digital Security in a Networked World* 2nd ed. (Hoboken, NJ: John Wiley & Sons, à paraître en 2004).
[216]Entrevue de Daniel Egger par David Berlind « Instead of indemnification, consider 'open source insurance' » *Tech Update Software Infrastructure* (18 février 2004), en ligne : ZDNet <http://techupdate.zdnet.com/techupdate/stories/main/open_source_insurance.html>.
[217]Schneier, *supra* note 215.

Il y a des preuves abondantes à l'appui de l'énorme croissance prévue dans le domaine de l'assurance cybernétique. Un sondage mondial sur la sécurité de l'information (Global Information Security Survey[218]) fait par Ernst et Young en 2003 a porté sur 1 400 compagnies. Seuls 7 % des répondants savaient qu'ils avaient une couverture d'assurance spécifique pour les risques touchant à l'Internet et aux réseaux. Près d'un tiers des répondants pensaient qu'ils étaient couverts pour ces risques, mais ils ne l'étaient pas en fait. Trente-quatre pour cent des répondants savaient qu'ils n'avaient pas de couverture et 22 % ont admis qu'ils n'étaient pas au courant de leur couverture. Pour Ernst et Young, le fait que seuls 7 % des répondants avaient une cyber-assurance était « … un pourcentage étonnamment faible, étant donné l'environnement de risque et le fait que les polices générales n'assurent pas une telle couverture ».

Ce faible taux de saturation, combiné à des responsabilités croissantes, rend presque certaine la croissance de la cyber-assurance. Il y a un certain nombre d'obstacles à la croissance de la cyber-assurance comme industrie, soit le manque de données actuarielles, le précédent (personne ne vous assurait pour les pannes de l'An 2000) et autres barrières. Peut-être que la demande du marché stimulera l'innovation nécessaire pour surmonter ces obstacles, mais il n'y a aucun doute que cette innovation sera un préalable à l'essor de l'industrie.

Et tout comme il y a des preuves de faibles taux de couverture, il y a également des preuves de l'augmentation des risques et des responsabilités. Les CERT® Centers au Software Engineering Institute de Carnegie Mellon University suivent les infractions ou les incidents de sécurité. Ils signalent que le nombre d'incidents est passé de 21 756 en 2000 à 82 094 en 2002, soit une augmentation de 377 %[219]. Il n'est pas étonnant que cette tendance se poursuive en 2003 et au début de 2004. Les dommages, à la fois directs et indirects, subis par les organisations ont augmenté en proportion. Même s'il n'y a pas de mesures définitives, il est certain que les dommages se chiffrent à de nombreux milliards de dollars annuellement dans le monde.

En résumé, la cyber-assurance peut et doit assurer :

- Le transfert des risques
- La définition des pratiques exemplaires pour la réduction des risques
- Des incitatifs pour l'adoption de ces pratiques exemplaires
- Une meilleure éducation

Le résultat de ces quatre éléments sera amélioré par la gestion des risques cybernétiques et cela pourrait se traduire directement par une infrastructure d'information essentielle plus solide.

[218]Ernst & Young, Global Information Security Survey 2003 (New York: Ernst & Young), en ligne : Ernst & Young <http://www.ey.com/global/download.nsf/US/TSRS_Global_Information_Security_Survey_2003/$file/TSRS_-_Global_Information_Security_Survey_2003.pdf >.

[219]CMU CERT® Coordination Center, Software Engineering Institute, Carnegie Mellon University, News Release (août 2003).

9.4.3 Aperçu des risques cybernétiques et de la cyber-assurance

Il y a des produits de cyber-assurance qui couvrent toute une variété de risques en matière d'infrastructure de l'information. Pour la plupart, il ne semble pas y avoir de polices types entre les diverses compagnies (les erreurs et omissions étant une exception notable). Chaque compagnie offre une sélection de polices qui couvrent un ou plusieurs risques cybernétiques. Ces risques/polices types comprennent ce qui suit : erreurs et omissions professionnelles, sécurité des réseaux, violation du droit d'auteur et contrefaçon de marque de commerce ou de brevet, destruction ou altération des données, coûts des relations publiques, remboursement des fonds versés pour information sur les crimes et extorsion sur l'Internet.

9.4.3.1 Erreurs et omissions professionnelles

L'assurance pour les erreurs et les omissions est le type le plus courant de cyber-assurance. La police en cas d'erreurs et omissions couvre le détenteur en cas d'actes négligents et d'omissions qui peuvent causer des préjudices à ses clients. Cette police porte en général sur le fonctionnement des systèmes et des logiciels personnalisés et, à un degré moindre, sur les services des technologies de l'information (TI). Elle traite d'éléments comme les erreurs de programmation ou la défaillance des logiciels ou des systèmes qui n'ont pas fonctionné comme promis dans le contrat. La couverture englobe à la fois les coûts de la défense en droit et les jugements rendus contre le fournisseur.

9.4.3.2 Sécurité des réseaux

Les atteintes à la sécurité des réseaux sont de plus en plus courantes et elles permettent aux attaquants ce qui suit :

- Transmettre et/ou installer du code malveillant comme des virus et des chevaux de Troie;
- Obtenir l'accès non autorisé aux données, ce qui peut entraîner des violations de la vie privée;
- Interrompre le service et provoquer des violations de contrat et
- Voler des données sensibles.

La cyber-assurance peut limiter à la fois les dommages de la première partie et de la partie tierce.

9.4.3.3 Violation du droit d'auteur et contrefaçon de marque de commerce ou de brevet

Comme il a été expliqué dans la section 9.1, on demande de plus aux fournisseurs d'indemniser leurs clients en cas de violation du droit d'auteur ou de contrefaçon de marque de commerce ou de brevet. Cette tendance s'explique par l'augmentation alarmante, au cours des dernières années, du nombre de poursuites dans ce domaine. Cette augmentation a été particulièrement évidente aux États-Unis. Il y a eu également une augmentation importante dans la valeur des jugements octroyés. Comme dans d'autres types de cyber-assurance, les polices couvrent en général à la fois les coûts de la défense et les jugements, jusqu'aux limites spécifiées.

Un second type de cyber-assurance a été offert dernièrement dans ce domaine. On l'appelle police de poursuite et cela aide à payer les frais juridiques de l'action en justice intentée contre un contrefacteur présumé.

9.4.3.4 Destruction ou altération des données

On peut soutenir que les données représentent le bien le plus important dans l'infrastructure d'information essentielle. Les systèmes peuvent être remplacés en général, bien que ce soit avec quelques difficultés. Les données sont souvent beaucoup moins remplaçables. La cyber-assurance peut limiter la perte financière résultant de la perte ou de l'altération de données due à un accident ou à une activité malveillante.

9.4.3.5 Coûts des relations publiques

De nombreux crimes et accidents cybernétiques associés à l'infrastructure d'information ne sont pas signalés par les victimes. L'une des principales raisons en est que les victimes s'inquiètent de perdre leur réputation auprès des clients, des investisseurs, des employés et des organismes de réglementation. Les conséquences financières peuvent être bien supérieures aux pertes directes dues à l'incident. Les initiatives de relations publiques après les incidents sont à la fois nécessaires et coûteuses.

9.4.3.6 Remboursement des fonds versés pour information sur des crimes

Si une organisation est victime d'un incident malveillant, il est parfois souhaitable d'offrir une récompense pour toute information menant à l'arrestation et à la condamnation de la ou des personnes responsables. Une telle récompense peut faire partie d'une initiative de relations publiques et aussi avoir un effet de dissuasion contre des incidents futurs. Par exemple, le Groupe SCO a offert récemment une récompense en relation avec le virus Mydoom[220]. Il est possible d'obtenir une cyber-assurance qui limitera le coût d'une telle récompense dans certaines circonstances

9.4.3.7 Extorsion sur Internet

L'extorsion cybernétique croît rapidement. La forme la plus courante est celle de la menace d'une attaque distribuée de déni de service qui mettra hors fonction le site Web de la victime. Les cibles les plus populaires sont les sites où il y a une forte perte par minute de temps d'immobilisation. Les sites Internet de jeux de hasard sont parmi les plus menacés[221]. Il est presque impossible de se défendre contre ces attaques si elles sont bien exécutées. Il y a eu récemment une attaque de déni de service sur le site Web du Groupe SCO. Les détails de l'attaque étaient connus d'avance, y compris l'heure précise de l'attaque. En dépit de cette connaissance préalable, l'attaque a désactivé le site.

9.4.4 ISO 17799

Dans la section 9.4.2, nous avons mentionné que l'un des principaux éléments qui seront pilotés par l'assurance est celui de la définition des pratiques exemplaires. Cela est déjà en train de se produire. L'un des principaux exemples est l'évolution du Code de pratique pour la gestion de la sécurité de l'information établi par l'Organisation internationale de normalisation (ISO) et que l'on désigne sous le nom de Norme ISO 17799. Cette norme de sécurité étendue traite

---

[220]Ken Mingis, « SCO Offers $250,000 Reward for Arrest of Mydoom Worm Author » *ComputerWorld* (27 janvier 2004), en ligne : ComputerWorld <http://www.computerworld.com/securitytopics/security/virus/story/0,10801,89470,00.html>.

[221]Paul Roberts, « Super Bowl fuels gambling sites' extortion fears » *InfoWorld* (29 janvier 2004), en ligne : InfoWorld <http://www.infoworld.com/article/04/01/29/HNsuperbowl_1.html>.

directement des pratiques en matière de sécurité cybernétique. Elle constitue la base des évaluations de sécurité en ligne et sur site qui sont menées par les compagnies d'assurance comme le Groupe AIG (American International Group). Le Groupe AIG souscrit 70 % des polices de cyber-assurance aux États-Unis ainsi qu'un grand nombre au Canada. Nous avons pensé qu'il serait utile de fournir un bref aperçu de la norme ISO 17799 pour donner un avant-goût de nombreuses autres normes qui, selon nous, évolueront à l'avenir. La description ci-dessous (dans sa version anglaise en bas de page) est tirée de Risk Associates[222] :

> L'ISO17799 est une norme de sécurité détaillée. Elle est organisée en dix chapitres importants, chacun d'eux couvrant un sujet ou un domaine différent :
>
> 1. Plan de continuité
> Les objectifs de ce chapitre sont les suivants : amortir les effets des interruptions des activités opérationnelles et des processus de travail essentiels en cas de pannes ou de sinistres majeurs.
>
> 2. Contrôle d'accès
> Les objectifs de ce chapitre sont les suivants : 1) contrôler l'accès à l'information; 2) empêcher l'accès non autorisé aux systèmes d'information; 3) assurer la protection des services en réseau; 4) empêcher l'accès non autorisé aux ordinateurs; 5) détecter les activités non autorisées; 6) assurer la sécurité de l'information en cas d'utilisation d'installations mobiles de téléréseautage et d'informatique.
>
> 3. Développement et maintenance
> Les objectifs de ce chapitre sont les suivants : 1) s'assurer que la sécurité est intégrée dans les systèmes opérationnels; 2) prévenir la perte, la modification ou la mauvaise utilisation des données de l'utilisateur dans les systèmes d'application; 3) protéger la confidentialité, l'authenticité et l'intégrité de l'information; 4) s'assurer que les projets et les activités de soutien des TI sont conduits de manière sécurisée; 5) assurer la sécurité des logiciels et des données des systèmes d'applications.
>
> 4. Sécurité de l'environnement et des biens physiques
> Les objectifs de ce chapitre sont les suivants : empêcher l'accès non autorisé, les dommages et les interférences dans les locaux et l'information de l'entreprise; prévenir les pertes, les dommages ou la compromission des biens et l'interruption des activités de l'entreprise; prévenir la compromission ou le vol de l'information et des installations de traitement de l'information.
>
> 5. Conformité
> Les objectifs de ce chapitre sont les suivants : 1) éviter les violations de toute loi criminelle ou civile, des obligations prévues par la loi, par la réglementation ou dans les contrats et de toutes les exigences en matière de sécurité; 2) assurer la conformité des systèmes avec les politiques et les normes organisationnelles en matière de sécurité et 3) maximiser l'efficacité et minimiser les interférences dans le processus de vérification des systèmes.
>
> 6. Sécurité du personnel
> Les objectifs de ce chapitre sont les suivants : réduire les risques d'erreur humaine, de vol, de fraude ou de mauvaise utilisation des installations; s'assurer que les utilisateurs

[222]Risk Associates, cité dans l'*ISO 17799 Service & Software Directory*, ISO 17799: What Is It?, (2004), en ligne : ISO 17799: What Is It? <http://www.iso17799software.com/what.htm>.

sont au courant des menaces et des risques en matière de sécurité de l'information et qu'ils sont en mesure d'appuyer la politique de sécurité de l'entreprise dans le cours de leur travail normal; minimiser les dommages dus à des incidents de sécurité et à des défectuosités et tirer des leçons de ces incidents.

7. Organisation de la sécurité
Les objectifs de ce chapitre sont les suivants : 1) gérer la sécurité de l'information au sein de la compagnie; 2) assurer la sécurité des installations organisationnelles de traitement de l'information et des biens d'information consultés par des tiers et 3) assurer la sécurité de l'information lorsque la responsabilité du traitement de l'information a été donnée en sous-traitance à une autre organisation.

8. Gestion des ordinateurs et des opérations
Les objectifs de ce chapitre sont les suivants : 1) assurer le fonctionnement correct et sûr des installations de traitement de l'information; 2) minimiser le risque des pannes de systèmes; 3) protéger l'intégrité des logiciels et de l'information; 4) assurer l'intégrité et la disponibilité dans le domaine du traitement de l'information et des communications; 5) assurer la protection de l'information dans les réseaux et la protection de l'infrastructure de soutien; 6) prévenir les dommages aux biens et les interruptions des activités de l'entreprise et 7) prévenir les pertes, les modifications ou la mauvaise utilisation de l'information échangée entre les organisations.

9. Classification et contrôle des biens
Les objectifs de ce chapitre sont les suivants : assurer la protection appropriée des biens de l'entreprise et s'assurer que les biens d'information reçoivent un niveau approprié de protection.

10. Politique de sécurité
Les objectifs de ce chapitre sont les suivants : fournir une orientation à la direction et appuyer la sécurité de l'information.

Chaque chapitre comprend les énoncés détaillés qui constituent la norme.

10.0 Mécanismes actuels ciblés en matière de responsabilité

Dans la section précédente, nous avons traité des mécanismes de responsabilité qui s'appliquent à tous les types de composants (produits logiciels, logiciels personnalisés, systèmes, services TI et matériel) qui constituent l'infrastructure d'information. Dans cette section, nous abordons les mécanismes de responsabilité qui s'appliquent essentiellement à un type de composant. Ces mécanismes sont traités dans les parties consacrées aux composants auxquels ils s'appliquent le mieux.

Dans les sections 10.1, 10.2 et 10.3, nous avons choisi assez arbitrairement trois points dans la gamme des logiciels qui ont des niveaux croissants de complexité dans le domaine de la responsabilité, soit les produits, les programmes personnalisés et les systèmes. Les différences entre ces points sont assez importantes pour changer la perception de la responsabilité d'un point à l'autre.

10.1 Produits logiciels

Le domaine de la vente des logiciels est fondamentalement différent d'autres domaines de plusieurs façons importantes dont quelques-unes ont des conséquences sur le plan juridique et de la responsabilité. Tout d'abord, le logiciel est caractérisé par de courts cycles de vie du produit (tout comme d'autres composants de l'infrastructure d'information essentielle). En partie à cause de cela, on ne peut pas produire le logiciel « parfait » (en effet, ce logiciel aura toujours quelques « bogues » ou erreurs). En second lieu, comme pour les autres produits informatiques, les circuits de distribution des logiciels sont compliqués et ils ont plusieurs facettes[223]. En troisième lieu, le logiciel n'est pas vendu. Il est plutôt utilisé sous licence.

La majorité des produits logiciels ont une durée de vie utile relativement brève (c'est-à-dire pour toute version spécifique du produit). Contrairement à de nombreux autres secteurs de l'industrie, il faut compter en semaines ou en mois, plutôt qu'en années, les progrès réalisés et les innovations lancées dans l'industrie du logiciel. En outre, cette industrie est caractérisée par un niveau élevé de concurrence alors qu'un bon nombre de nouveaux produits sont constamment mis sur le marché. Tout cela, combiné aux courts cycles des produits, a fréquemment pour résultat des attentes excessives de manière déraisonnable de la part de l'utilisateur final. Les fournisseurs de logiciels, qui subissent la pression constante de rester en tête de la concurrence, affirment souvent que les utilisateurs achètent de nouveaux produits et des mises à niveau pour avoir de meilleures fonctions plutôt qu'une plus grande qualité et fiabilité[224].

La création du logiciel suit essentiellement plusieurs étapes distinctes, à partir de la première étape de planification et de conception au niveau général, en passant par la rédaction du code et donc des instructions et déclarations jusqu'à l'étape finale des tests qui sert à découvrir et à

---

[223]Takach, *supra* note 192 à 423.

[224]Aaron Ricadela, « The State of Software Quality », *Information Week.com News*, (21 mai 2001), en ligne : site Web Information Week http://www.informationweek.com/shared/printHTMLArticle.jhtml?article=/838/quality.htm> [Ricadela, « Software Quality »].

corriger autant d'erreurs que possible avant de fournir le produit à l'utilisateur final[225]. Même si la plupart des logiciels subissent une quantité importante de tests, c'est un fait accepté parmi les programmeurs et les développeurs qu'il est pratiquement impossible de découvrir et d'éradiquer toutes les erreurs avant la sortie du produit. En dépit des bonnes intentions, le code défectueux est toujours l'épouvantail de l'industrie du logiciel. Selon le Groupe Standish (firme spécialisée dans les études de marché), on pouvait attribuer jusqu'à 45 % du temps d'immobilisation des systèmes informatiques à un mauvais code, ce qui a coûté aux compagnies américaines plus de 100 milliards de dollars en réparations et pertes de productivité (chiffres de l'an 2000)[226]. Il convient de noter que ce chiffre de 100 milliards de dollars ne comprend pas le coût de la perte de clients mécontents. Selon Alan Willett, ingénieur en processus logiciel à Xerox Corp., « absolument, les produits logiciels commerciaux que nous achetons n'ont pas la qualité dont nous avons besoin »[227].

Même s'il était possible de concevoir du logiciel exempt d'erreurs[228], son coût serait tellement prohibitif et il prendrait tellement de temps qu'il ne serait pas faisable commercialement à la lumière de l'environnement commercial actuel. Ainsi, l'un des mécanismes actuels de responsabilité est celui des programmes de support offerts à l'utilisateur par les fournisseurs de logiciels. Ces programmes ont un élément important de correction des erreurs qui se manifestent une fois que le client a commencé à utiliser le produit logiciel. Un autre aspect de ce programme de support logiciel typique destiné à l'utilisateur final est celui de la fourniture des versions ou mises à niveau futures du logiciel. Même si la principale *raison d'être* de ces versions ultérieures consiste à fournir au client des fonctions additionnelles et/ou améliorées, ces mises à niveau servent également de véhicule pour la distribution de nouvelles copies du logiciel antérieur dont certains bogues ont été retirés[229].

10.1.1 Limitations de responsabilité et exclusions de garantie

Le logiciel qui est créé pour la distribution sur le marché de masse (par opposition au logiciel personnalité) comprend en général les modalités de la licence ainsi que diverses exclusions de la garantie et limitations de la responsabilité (invariablement en faveur du fournisseur du logiciel). À titre d'exemple, des parties pertinentes du Contrat de licence de logiciel de Apple Computer, Inc.[230] et du Contrat de licence de l'utilisateur final de Microsoft[231] sont reproduites ci-dessous :

---

[225]Takach, *supra* note 192 à 425.
[226]Ricadela, « Software Quality », *supra* note 223.
[227]*Ibid*.
[228]Les définitions de mauvais logiciel varient, mais il est généralement admis qu'il suffit de trois à quatre défauts par 1 000 lignes de code pour donner un programme à la performance médiocre. À chaque rédaction de dix lignes de code, le programmeur moyen commet une erreur. Lorsqu'on considère que de nombreuses applications logicielles commerciales contiennent des millions ou des dizaines de millions de lignes de code et que les fournisseurs de logiciels doivent débourser au moins 50 % de leurs budgets de développement pour corriger les erreurs pendant la phase d'essai, la portée énorme du problème devient apparente.
[229]Takach, *supra* note 192 à 426.
[230]Apple Computer, Inc. Software License Agreement (3 décembre 2003), en ligne : Apple Computer, Inc. Support - Software License Agreement <http://docs.info.apple.com/article.html?artnum=26275>.
[231]Microsoft, Inc., END-USER LICENSE AGREEMENT FOR MICROSOFT SOFTWARE - TrueType core fonts for the Web EULA (28 décembre 2001), en ligne : Microsoft Typography <http://www.microsoft.com/typography/fontpack/eula.htm>.

CONTRAT DE LICENCE MONO-UTILISATION DE APPLE COMPUTER, INC.

LISEZ ATTENTIVEMENT CE CONTRAT DE LICENCE DE LOGICIEL (« LICENCE ») AVANT D'UTILISER LE LOGICIEL. EN UTILISANT CE LOGICIEL, VOUS ACCEPTEZ LES TERMES DE CETTE LICENCE.

6. Exclusion de garanties. VOUS RECONNAISSEZ ET ADMETTEZ EXPRESSÉMENT QUE L'UTILISATION DU LOGICIEL APPLE EST À VOS RISQUES ET PÉRILS ET QUE LA TOTALITÉ DU RISQUE RELATIF À LA QUALITÉ, AUX PERFORMANCES, À L'EXACTITUDE ET AU MANIEMENT SATISFAISANTS REPOSE SUR VOUS. À L'EXCEPTION DE LA GARANTIE LIMITÉE DES SUPPORTS STIPULÉE CI-DESSUS ET DANS LES LIMITES MAXIMALES AUTORISÉES PAR LA LÉGISLATION EN VIGUEUR, LE LOGICIEL APPLE EST FOURNI « TEL QUEL »AVEC TOUS SES DÉFAUTS ET SANS AUCUNE GARANTIE D'AUCUNE SORTE. APPLE ET LES CONCÉDANTS D'APPLE (DÉSIGNÉS COLLECTIVEMENT PAR L'EXPRESSION « APPLE » AUX FINS DES DISPOSITIONS DES PARAGRAPHES 6 ET 7) EXCLUENT PAR LA PRÉSENTE LICENCE LA TOTALITÉ DES GARANTIES ET CONDITIONS, EXPLICITES, TACITES OU LÉGALES, Y COMPRIS DE FAÇON NON LIMITATIVE LES GARANTIES ET/OU CONDITIONS IMPLICITES DE QUALITÉ MARCHANDE, DE QUALIT É SATISFAISANTE, D'ADÉQUATION À UN OBJECTIF PARTICULIER, D'EXACTITUDE, DE SÉRÉNITÉ D'UTILISATION ET DE NON-EMPIÉTEMENT SUR LES DROITS DE TIERCES PARTIES, LE TOUT À L'ÉGARD DU LOGICIEL APPLE. APPLE NE GARANTIT NULLEMENT L'ABSENCE DE PERTURBATIONS LORS DE VOTRE UTILISATION DU LOGICIEL APPLE, QUE LES FONCTIONS CONTENUES DANS LE LOGICIEL APPLE CORRESPONDRONT À VOS BESOINS, QUE LE FONCTIONNEMENT DU LOGICIEL APPLE SERA ININTERROMPU OU EXEMPT D'ERREUR, OU QUE TOUT DÉFAUT DU LOGICIEL APPLE SERA CORRIGÉ. AUCUNE INFORMATION NI AUCUN CONSEIL COMMUNIQUÉS VERBALEMENT OU PAR ÉCRIT PAR APPLE OU PAR L'UN DE SES REPRÉSENTANTS AUTORISÉS NE POURRA CONSTITUER UNE GARANTIE. SI LE LOGICIEL APPLE S'AVÉRAIT DÉFECTUEUX, VOUS ASSUMERIEZ SEUL LE COÛT TOTAL DE TOUTE RÉVISION, RÉPARATION OU RECTIFICATION NÉCESSAIRES. CERTAINES LÉGISLATIONS NE PERMETTANT NI L'EXCLUSION DE GARANTIES IMPLICITES, NI LES RESTRICTIONS AUX DROITS EN VIGUEUR DES CONSOMMATEURS, IL EST POSSIBLE QUE L'EXCLUSION ET LES LIMITES MENTIONNÉES CI-DESSUS NE VOUS CONCERNENT PAS.

7. Limitation de responsabilité. DANS LA MESURE OÙ LA LÉGISLATION NE L'INTERDIT PAS, EN AUCUN CAS APPLE NE SERA RESPONSABLE DE DOMMAGE CORPOREL NI DE QUELCONQUE DOMMAGE ACCIDENTEL, SPÉCIAL, INDIRECT OU ACCESSOIRE, Y COMPRIS DE FAÇON NON LIMITATIVE, LES DOMMAGES DUS AUX PERTES DE BÉNÉFICES, PERTES DE DONNÉES, INTERRUPTION DES ACTIVITÉS OU TOUT AUTRE DOMMAGE COMMERCIAL OU PERTE COMMERCIALE RÉSULTANT DE OU RELATIFS À VOTRE UTILISATION OU VOTRE INAPTITUDE À UTILISER LE LOGICIEL APPLE, QUELLE QU'EN SOIT LA CAUSE, SANS TENIR COMPTE DE LA THÉORIE DE LA RESPONSABILITÉ (QUE CE SOIT POUR RUPTURE DE CONTRAT, EN RESPONSABILITÉ CIVILE, OU AUTRE) ET MÊME SI APPLE A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES. CERTAINES JURIDICTIONS NE PERMETTANT PAS LA LIMITATION DE RESPONSABILITÉ

POUR DOMMAGES PERSONNELS, INDIRECTS OU ACCESSOIRES, IL EST POSSIBLE QUE CETTE LIMITATION NE VOUS CONCERNE PAS. La responsabilité totale d'Apple envers vous au titre de tout dommage (en dehors de ce que la législation pourrait exiger dans les cas impliquant une blessure) n'excédera en aucun cas la somme de cinquante dollars (50 $). Les limitations susdites s'appliqueront même si le recours indiqué ci-dessus fait défaut à sa vocation essentielle.

CONTRAT DE LICENCE UTILISATEUR FINAL POUR LOGICIEL MICROSOFT

IMPORTANT – À LIRE ATTENTIVEMENT : Ce Contrat de Licence Utilisateur Final Microsoft (le « CLUF ») est un accord entre vous (personne physique ou personne morale unique) et Microsoft Corporation, applicable au produit logiciel Microsoft identifié ci-dessus, qui inclut une documentation « en ligne » ou électronique et qui peut inclure aussi des programmes d'ordinateur, des supports associés, et une documentation imprimée (le « PRODUIT LOGICIEL » ou « LOGICIEL »). En installant, en copiant, ou en utilisant de quelque autre manière le PRODUIT LOGICIEL, vous reconnaissez être lié par les termes du présent CLUF. Si vous êtes en désaccord avec les termes de ce CLUF, vous n'êtes pas autorisé à utiliser ce PRODUIT LOGICIEL.

EXCLUSION DE GARANTIE. Microsoft exclut expressément toute garantie relative au PRODUIT LOGICIEL. Le PRODUIT LOGICIEL et la documentation y afférente sont fournis « en l'état », sans garantie d'aucune sorte, expresse ou implicite, notamment sans aucune garantie implicite de qualité, d'adéquation à un usage particulier ou d'absence de contrefaçon. Vous assumez l'ensemble des risques découlant de l'utilisation ou des performances du PRODUIT LOGICIEL.

ABSENCE DE RESPONSABILITÉ POUR LES DOMMAGES INDIRECTS. Microsoft ou ses fournisseurs ne pourront, en aucun cas, être tenus pour responsables de quelque dommage que ce soit (notamment des pertes de bénéfices, des interruptions d'activité, des pertes d'informations commerciales ou de toute autre perte pécuniaire), résultant de l'utilisation ou de l'impossibilité d'utiliser ce produit Microsoft, alors même que Microsoft aurait été informée de l'éventualité de tels dommages. Certains pays ou certaines juridictions n'autorisent pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, de sorte que la limitation ci-dessus peut ne pas vous être applicable.

Les paragraphes reproduits ci-dessus sont représentatifs de presque tout le logiciel commercial. Comme on peut le voir, la responsabilité en matière de produits est pratiquement inexistante. Les lois qui régissent la vente des produits datent d'environ 100 ans. Les lois sur les ventes dans les provinces canadiennes de la common law suivent le modèle de la loi originale anglaise *Sale of Goods Act* qui visait à codifier les lois de vente s'appliquant aux objets produits dans les usines anglaises vers la fin des années 1800. Ainsi, il n'est pas illogique que ces lois sur la vente d'objets ne soient pas compatibles avec les problèmes soulevés par les ventes des logiciels d'ordinateur. À toutes fins utiles, ces lois portent sur la vente de biens tangibles et elles ne règlent souvent pas les questions entourant les biens intangibles comme les logiciels et autres produits d'information, particulièrement lorsque le logiciel n'est pas « vendu », mais qu'il est plutôt mis sous licence. À cause de cela, la plupart des fournisseurs de logiciels déclinent expressément toute responsabilité dans les conditions et garanties de leurs contrats de licence.

De nombreux fournisseurs de logiciels soutiennent que l'utilisateur final cause un bon nombre de ses propres problèmes en personnalisant fortement ses produits d'application logiciels[232]. Étant donné que les fournisseurs savent que le logiciel peut être utilisé de bien des façons différentes par l'acheteur, ils indiquent une limitation générale de responsabilité dans le contrat de vente avec l'utilisateur. Ils limitent ainsi leur responsabilité à un montant fixe pour les dommages directs et ils excluent tous les autres dommages, comme les pertes de profits et les dommages indirects. En outre, les tribunaux n'ont pas voulu, dans des situations très variées, imposer une responsabilité illimitée aux fournisseurs des produits et services d'information, y compris le logiciel, particulièrement dans le cas de perte économique pure[233].

Il est intéressant de noter que la plupart des logiciels sont produits par des équipes composées de diverses personnes plutôt que par des programmeurs qui travaillent tout seuls. C'est important car la tâche d'attribuer la responsabilité des problèmes inhérents au logiciel s'exacerbe et s'obscurcit. La responsabilité des fautes, qui incombe traditionnellement à une seule personne, ne s'extrapole pas facilement à des groupes collectifs[234]. Même si ce problème de la responsabilité collective (appelé aussi « le problème de nombreuses mains ») n'est pas propre au logiciel lui-même, il est extrêmement pertinent puisque la plupart des logiciels sont produits dans des cadres institutionnels. (La responsabilité collective est un problème qui afflige d'autres technologies, ainsi que de grandes sociétés, des gouvernements et les forces militaires.)

Un autre aspect de ce problème de responsabilité est lié au fait que le logiciel est fréquemment assemblé à partir de modules ou de segments. Il peut inclure du code provenant de versions précédentes ou utiliser du code provenant de logiciels entièrement différents. En ce qui concerne le logiciel qui a évolué au point d'avoir un niveau élevé de complexité, une personne à elle seule ne peut pas comprendre tout le programme et encore moins tenir registre de tous ceux qui ont contribué à ses divers composants. Ainsi, la responsabilité des erreurs ou des mauvais fonctionnements est encore plus obscurcie[235]. (Par exemple, la version initiale de Microsoft Windows 2000 contenait environ 40 millions de lignes de code. Étant donné que la norme de l'industrie pour le logiciel produit par les compagnies comme Microsoft accepte un bogue ou un défaut connu par 1 500 lignes de code, on pourrait s'attendre à avoir environ 600 000 bogues dans le programme[236].)

---

[232]Ricadela, *supra* note 224.
[233]Takach, *supra* note 192 à 477-480.
[234]Helen Nissenbaum, « Computing and Accountability », (1994) 37 *Communications of the ACM 72*.
[235]*Ibid*.
[236]« Changes in the Customer Support Industry » *Computer News* (janvier 1999), en ligne : Help Desk Solutions, Inc. <http://www.helpdesksolutions.com/Publications/change_support.htm >.

10.1.2 Quelques points de vue divergents sur l'attribution de la responsabilité dans le domaine du logiciel

La question de savoir si l'attribution de la responsabilité qui prévaut est appropriée (comme entre les fabricants et les consommateurs de logiciels) continue de faire l'objet de débats considérables[237]. Le manque de consensus et les positions très différentes prises par divers commentateurs sur cette question illustrent fortement la nécessité d'avoir un cadre systématique de discussion, y compris des données empiriques fiables pour éclairer les débats. Des arguments selon lesquels cette attribution de la responsabilité peut ou devrait être changée à l'aide de mécanismes du secteur privé ou du secteur public, ou d'une combinaison des deux, deviennent pertinents dans un certain nombre de circonstances. Celles-ci incluent le moment où la question de l'attribution de la responsabilité due à des violations de sécurité fait surface et le moment où ces violations portent sur des questions de fiabilité du logiciel.

Par exemple, un auteur[238] soutient qu'il n'est pas pratique pour les consommateurs de créer leur propre logiciel de sécurité. Il déclare en outre qu'il est raisonnable que les fabricants soient responsables de la fiabilité de leurs produits.

D'autres auteurs[239] soutiennent que le fait d'imposer la responsabilité n'est pas l'outil approprié pour réduire le nombre et la gravité des événements, contraires à la sécurité, causés par des problèmes de logiciel. Selon ce raisonnement, le logiciel devrait être traité différemment des autres produits (par exemple, les automobiles). Parmi les raisons citées, nous trouvons :

1. La durée de vie utile prévue relativement courte de nombreux produits logiciels par rapport au temps requis pour régler un différend devant les tribunaux (c'est-à-dire que le logiciel sera désuet avant que l'affaire ne soit finalement réglée);
2. Le fabricant ne peut pas raisonnablement prévoir les buts pour lesquels le logiciel sera utilisé; et
3. S'il fallait imposer la responsabilité aux fabricants de logiciels, un bon nombre d'entre eux quitteraient le marché et cela réduirait alors le degré et le rythme de l'innovation.

Des deux côtés de ce débat, on invoque, au moins implicitement, des exemples standard du raisonnement économique. On fait des suppositions au sujet de l'état du marché, ou du résultat probable des changements, que l'on peut tester empiriquement jusqu'à un certain degré.

De toute façon, ce débat au sujet de l'attribution appropriée de la responsabilité aux fabricants de logiciels, pour les dommages dus à des incidents contraires à la sécurité causés par des insuffisances du logiciel, est un sous-ensemble du problème suivant. La question plus générale concerne l'attribution appropriée de la responsabilité à la fois aux fabricants de logiciels et du

---

[237]Voir, par exemple, Nancy R. Mead, *International Liability Issues for Software Quality*, Special Report, CERT Research Center, CMU/SEI-2003-SR-001, (juillet 2003) à 19, en ligne : Carnegie Mellon Software Engineering Institute <http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03sr001.pdf>.

[238]Daniel J. Ryan, « Two Views on Security Software Liability: Let the Legal System Decide ». IEEE Security & Privacy 1, 1 (2003): 70-72.

[239]Voir, par exemple, Carey Heckman, « Two Views on Security Software Liability: Using the Right Legal Tools ». IEEE Security &Privacy 1, 1 (2003): 70-72, en ligne : <http://csdl2.computer.org/dl/mags/sp/2003/01/j1073.htm>.

matériel pour les dommages subis en relation avec divers types d'événements, que ce soit ou non des événements contraires à la sécurité.

Nous pensons que ce débat pourrait profiter de l'application rigoureuse du raisonnement économique standard. Même si cette analyse est en dehors de la portée du présent rapport, nous estimons qu'il peut être prudent et efficace, au moment de faire cette analyse, d'intégrer les données qui sont recueillies à partir des diverses recherches proposées dans le présent document.

10.2 Logiciel personnalisé

10.2.1 Définition du logiciel personnalisé

Le logiciel personnalisé, appelé parfois programmation sur mesure, se fonde sur les exigences spécifiques d'une organisation. Aujourd'hui, il n'y a presque pas de logiciel personnalisé qui soit entièrement original. Des éléments de travaux antérieurs sont réutilisés pour accroître la productivité. En général, il y a un niveau plus élevé d'attente car on pense que le logiciel personnalisé répondra mieux aux besoins des acheteurs que les produits logiciels. Le logiciel personnalité représente une partie importante de l'infrastructure d'information.

10.2.2 Contrats de développement du logiciel

Nous nous sommes limités à examiner les mécanismes de responsabilité qui entrent en jeu lorsque le logiciel personnalisé est développé pour une organisation qui l'utilisera (l'acheteur) par une partie non liée (le fournisseur). Du logiciel personnalisé est encore développé à l'interne par les employés de l'organisation qui l'utiliseront par la suite. Nous n'avons pas étudié les mécanismes de responsabilité qui régissent ce logiciel personnalisé. Ces mécanismes sont extrêmement variables et souvent mal définis.

Le contrat de développement de logiciels documente un accord conclu entre un acheteur et un fournisseur pour que ce dernier bâtisse et développe une application ou un système requis par l'acheteur conformément à des spécifications mutuellement acceptables. Les mécanismes de responsabilité pour le logiciel personnalisé sont inscrits dans le contrat.

Les principales dispositions du contrat sur la responsabilité comprennent ce qui suit :

- Portée du travail, y compris des spécifications fonctionnelles et techniques
- Indemnisation contre toute violation de la propriété intellectuelle (IP)
- Jalons, dates d'échéance et clauses de pénalité associées
- Critères d'acceptation
- Procédures des tests d'acceptation
- Services préalables et postérieurs à la mise en œuvre

La plupart des contrats sur les logiciels personnalisés ont une composante de services. Cela comprend souvent la mise en œuvre, l'intégration, la formation et le support. Nous traitons de ces services dans la section 10.4.

10.2.3 Comment le régime de responsabilité échoue

Des efforts considérables ont été consacrés à la rédaction de contrats de logiciels personnalisés. Ces contrats régissent les milliers d'initiatives de développement de logiciels personnalisés qui ont été lancées. Par conséquent, nous avons un énorme bassin de connaissances au sujet de ce qui fonctionne (et de ce qui ne fonctionne pas) dans l'attribution et l'application des responsabilités. De nombreux problèmes sont attribuables à une source courante : l'incapacité à la fois du fournisseur et de l'acheteur de mettre suffisamment d'efforts et de ressources dans la phase de la relation préalable au contrat de développement.

L'un des problèmes les plus fréquents se produit lorsque les deux parties n'ont pas une compréhension claire et commune de ce qui est requis par l'acheteur. Cette compréhension ne peut sans doute avoir lieu que si les exigences sont décrites en détail dans le contrat au moment de la signature. Bien souvent, dans la hâte de voir les projets lancés, les contrats sont signés avec des annexes « à établir ». Ces annexes peuvent englober des éléments contractuels clés comme les spécifications techniques et les calendriers du projet. C'est une véritable recette de catastrophe. Étonnamment peut-être, le développement de spécifications fonctionnelles et techniques détaillées est extrêmement difficile, comme le prouve le nombre de fois où il n'est pas fait.

Un autre problème courant de responsabilité survient lorsque les procédures des tests d'acceptation des modules, du système global et de l'acceptation finale ne sont pas adéquatement spécifiées dans le contrat. Des différends se produisent fréquemment lorsque des accords sur ces procédures sont absents.

Le retard par rapport au calendrier établi entraîne souvent l'échec des projets de développement de logiciels personnalisés. Les fournisseurs et les acheteurs succombent souvent à la pression de s'entendre sur des délais prédéfinis, même si ces délais ne sont ni nécessaires ni réalistes. La tension qui en résulte peut pousser les gens à couper les coins ronds et mène finalement au chaos.

Les modalités de paiement peuvent créer des problèmes importants. Si les fournisseurs sont payés sur une base de temps et de matériaux, il y a un décalage inhérent des objectifs entre le fournisseur et l'acheteur.

Une dernière situation qui vaut la peine d'être mentionnée est celle des fournisseurs qui trouvent à l'occasion qu'ils ne peuvent tout simplement pas fournir le logiciel selon les exigences du contrat. Les fournisseurs doivent souvent se retirer des affaires ou ils n'ont pas les biens ni les capacités pour corriger les lacunes. Les problèmes qui sont décelés quelque temps après la fin du contrat sont souvent très difficiles à rectifier à cause d'une documentation médiocre ou parce qu'on n'a plus accès au talent original.

10.3 Systèmes

10.3.1 Définition des systèmes

L'infrastructure d'information se compose de nombreuses couches de systèmes interconnectés. Ces systèmes peuvent être des composants standard ou personnalisés ou encore des groupes de composants. Le processus de constitution des systèmes est appelé intégration des systèmes.

L'intégration des systèmes comprend la conception des architectures du système, l'identification des produits matériels et logiciels qui seront incorporés au système, l'identification des points d'interface entre les éléments du système et leurs spécifications détaillées, l'établissement du code personnalisé qui connecte les éléments du système et les tests de tout le système pour s'assurer que ce système respecte les spécifications établies.

Au début, l'intégration des systèmes était un processus très manuel et fortement personnalisé. Les composants n'étaient pas conçus pour fonctionner ensemble. Atteindre ce but était difficile. En réponse à la demande du marché, du logiciel d'intégration a été développé pour faciliter le travail d'assemblage des composants en un système fonctionnel. Ce logiciel d'intégration traditionnel, appelé logiciel intermédiaire ou intergiciel, servait à relier des applications commerciales ou personnalisées. Même s'il était coûteux et difficile à utiliser, le logiciel intermédiaire a été une amélioration considérable par rapport à une intégration entièrement manuelle.

Nous voyons maintenant l'émergence d'une nouvelle classe de produits qui rendent l'intégration des systèmes beaucoup plus facile en tirant parti des nouvelles normes multi-plateformes comme les services Web, le langage de balisage extensible XML et l'architecture de connexion Java. Gartner appelle ces produits des bus de service d'entreprise ESB (Enterprise Service Buses). Ces ESB sont définis comme « une nouvelle architecture qui exploite les services Web, le logiciel intermédiaire de messagerie, le routage intelligent et la transformation. Les ESB agissent comme un réseau d'intégration léger et omniprésent à travers lequel circulent les services logiciels et les composants d'application[240]. »

À mesure que l'intégration des systèmes devient plus facile et plus abordable, la demande continue de croître. Les organisations veulent que leurs systèmes soient connectés en temps réel à l'infrastructure d'information globale et elles ont besoin de cette connexion.

10.3.2 Principales normes d'intégration

Des normes clés sont en train d'accélérer le rythme d'intégration des systèmes et elles permettent en même temps aux utilisateurs d'établir des stratégies d'intégration qui ne dépendent pas d'un seul fournisseur. Voici quelques-unes de ces normes :

1. L'architecture de connexion Java (Java Connector Architecture) traite le premier problème qui consiste à introduire l'information dans les applications ou à l'extraire. Cela donne une seule norme qui complète les normes existantes comme

[240]Roy Schulte, Gartner Inc., cité par Ronan Bradley, « The Universal Enterprise Service Bus », PolarLake JIntegrator White Paper (3 janvier 2004), en ligne : PolarLake <http://www.polarlake.com/products/jintegrator/whitepaper/>.

la norme de connectivité de base de données Java JDBC (Java Database Connectivity) ou la norme d'appel RMI (Remote Method Invocation) et une vaste gamme d'interfaces de programmes d'application API (Application Program Interfaces) qui offrent un bon point de départ.

2. XML cherche à régler le plus gros problème de tout projet d'intégration : comment mettre le message dans le bon format pour sa prochaine destination? Même si la norme XML n'élimine pas la nécessité de transformer les messages, elle a diminué de façon importante la complexité associée à cette transformation.
3. Les services Web offrent des interfaces normalisées entre les applications ainsi que la possibilité d'une orchestration standardisée.
4. Le service de messagerie Java JMS (Java Messaging Service) fournit le protocole de communication asynchrone avec l'avantage additionnel de la prestation garantie des fonctions de publication/d'abonnement qui sont en général offertes par les produits de messagerie supportés par JMS comme WebSphere-MQ d'IBM[241].

10.3.3 Contrats d'intégration des systèmes

Les travaux d'intégration des systèmes sont généralement régis par des contrats qui contiennent des dispositions très semblables à celles du développement de logiciels personnalisés. Toutefois, il y a certaines différences.

Les projets d'intégration des systèmes donnent souvent des systèmes qui ont une portée et un impact très grands sur l'organisation de l'acheteur. Par conséquent, le fournisseur est souvent tenu partiellement responsable des résultats de l'entreprise et non pas tout simplement de la fonctionnalité. Les clauses sur le rendement des fournisseurs peuvent comporter des éléments comme les gains réalisés et l'augmentation des revenus.

À cause de la complexité des travaux d'intégration des systèmes, la clarté dans la définition des exigences prend une importance d'autant plus grande. Les exigences englobent de plus en plus d'éléments. Les fournisseurs ne peuvent pas ignorer sciemment les exigences opérationnelles.

Les produits matériels et logiciels sont fréquemment incorporés aux projets d'intégration des systèmes. Dans les contrats, il faut savoir à qui appartiennent ces produits (et qui paient pour eux) au cas où le contrat serait résilié rapidement et que le système ne serait jamais terminé.

10.3.4 Comment les projets échouent

Ici encore, il y a de nombreuses similitudes entre la façon dont les travaux d'intégration des systèmes échouent et la façon dont les projets de développement de logiciels personnalisés échouent. Mais, comme pour les contrats, il y a certaines différences.

Les fournisseurs montrent souvent de la réticence à assumer la responsabilité associée aux représentations et aux garanties de rendement (des performances) du système global. Un tel

[241] *Ibid*.

rendement est difficile à prévoir d'avance à cause de la complexité de l'interaction entre les composants. En outre, il n'est peut-être pas possible de corriger les lacunes de rendement à l'aide de l'architecture et des composants choisis. Comme il n'y a souvent aucune responsabilité claire, le système résultant risque de ne pas fournir les avantages souhaités par l'acheteur.

La plupart des composants des systèmes typiques sont des produits standard. De nouvelles versions de ces produits sortent constamment sur le marché. Cela se produit à la fois pendant les phases de développement et de mise en œuvre et à la post-implantation. Il est pratiquement impossible de prévoir l'impact de l'installation des nouvelles versions de composants. Les fournisseurs d'intégration des systèmes sont forcés d'adopter des solutions de rechange pour faire face à des fonctions non documentées relevées pendant les projets. Ces fonctions peuvent changer dans les versions ultérieures et elles peuvent avoir un impact négatif sur le système. Dans le cas du développement de logiciels personnalisés, le fournisseur peut exercer un contrôle important sur l'environnement de développement et ces types de problèmes sont beaucoup plus rares.

10.4 Services des technologies de l'information

De nombreux fournisseurs de services internes offrent autant qu'ils le peuvent avec les ressources qui sont à leur disposition. Un budget est établi pour le service et alors le groupe chargé du service voit ce qu'il peut fournir avec les ressources qu'il a. C'est ce qui se produit dans la plupart des services internes des organisations. C'est également ce qui se produit dans la plupart des groupes chargés des services internes des technologies de l'information (TI). C'est le genre de responsabilité où l'on s'engage à faire « tout son possible », ce qui est assez facile et de plus en plus contesté.

10.4.1 Bibliothèque de l'infrastructure des technologies de l'information (BITI/ITIL)

Il y a une nouvelle norme internationale sur la gestion des services TI. Cette norme se fonde sur la Bibliothèque de l'infrastructure des technologies de l'information (BITI, aussi appelée ITIL ou Information Technology Infrastructure Library)[242]. Cela a commencé en 1989 au Royaume-Uni lorsque le gouvernement a décidé de réunir une collection utile des meilleures pratiques pour appuyer et fournir les services TI, d'où la partie Bibliothèque de l'appellation. Le but était de fournir un outil pour aider les gouvernements à améliorer la façon dont les services TI étaient obtenus.

Aujourd'hui, la BITI est appuyée par un forum international d'utilisateurs, soit le Forum sur la gestion des services en technologies de l'information ou itSMF[243]. Il y a une section active du Forum itSMF[244] au Canada (on l'appelle parfois FGStica) avec des chapitres partout au pays. Plusieurs unités du gouvernement fédéral canadien ont adhéré au Forum itSMF Canada, tout comme plusieurs gouvernements provinciaux[245]. La BITI est en train de devenir une norme

[242]Il y a une grande documentation, toujours croissante, au sujet de la BITI (ITIL). Voir en ligne : <http://www.ogc.gov.uk/index.asp?id=2261> comme indicateur initial utile des ouvrages à consulter.
[243]Voir en ligne : IT Service Management Forum <http://www.itsmf.com/>.
[244]Voir en ligne : itSMF Canada <http://www.itsmf.ca>.
[245]Voir en ligne la liste récente des membres d'affaires de itSMF Canada : <http://www.itsmf.ca/corporate.asp>.

internationale. BS 15000[246] est la norme britannique connexe – « BS 15000 est la première norme mondiale sur la gestion des services TI … et elle se fonde énormément sur le cadre de travail de la BITI (ITIL ou IT Infrastructure Library)[247]. »

La BITI a établi la norme de responsabilité en matière de services TI. Son adoption est loin d'être universelle, mais elle a été utilisée assez largement pour savoir qu'elle fonctionne au Canada. Cette section présente le concept de responsabilité dans les services TI, tel qu'il est perçu dans le cadre BITI. Pour que le régime de responsabilité soit efficace, il faut avoir une norme en fonction de laquelle on peut mesurer et évaluer les performances. Dans le cadre de la BITI, les accords sur les niveaux de service fournissent cette référence.

10.4.2 Accords sur les niveaux de service

La BITI suppose qu'il y a deux parties dans un service TI. Il y a le fournisseur du service TI et le client du service TI. Le fournisseur et le client peuvent être tous deux dans la même organisation, mais il est utile de les traiter comme des parties distinctes. L'accord sur les niveaux d'un service TI est l'entente contractuelle entre le fournisseur et le client qui définit exactement ce qui doit être fourni, comment, où, quand, dans quelles conditions et d'après quelles suppositions.

La table des matières complète d'un accord sur les niveaux de service devrait inclure les éléments suivants[248] :

- La description des services à fournir
- Les engagements sur le plan des performances, avec le suivi et les rapports
- Les procédures à suivre pour la gestion des problèmes
- La description complète des frais et des dépenses permises
- Les obligations et les responsabilités du client
- La sécurité, la sauvegarde, la reprise et la continuité
- Les garanties offertes et les corrections possibles
- Les droits de la propriété intellectuelle et la confidentialité
- La conformité contractuelle et la résolution des différends
- Les procédures à suivre en cas de résiliation

Lorsque les deux parties sont dans la même organisation (ce qui est généralement le cas avec des services TI internes), bon nombre de ces éléments peuvent être couverts par des contrats types. Le but n'est pas de produire un gros document qui couvre de façon exhaustive chacun des services TI, mais plutôt d'établir des responsabilités claires entre le fournisseur et le client. Un accord interne sur les niveaux de service peut tenir sur une page de note de service et indiquer ce qui doit être fourni et à qui sont attribuées les responsabilités.

---

[246]Voir en ligne : BS15000 – The BS 15000 IT Service Management Standard <http://www.bs15000.org.uk/>.
[247]*Ibid.*
[248]Cette liste est établie d'après la trousse d'outils « Service Level Agreement Toolkit », EasyTec Solutions, 2002.

On peut soulever plusieurs points sur la façon dont cette approche fonctionne en pratique[249]. Le premier point essentiel est le suivant : si un aspect d'un service TI n'est pas mesuré, c'est donc qu'il n'est véritablement pas si important. Les gens font attention à ce qui est mesuré et il est courant de trouver des fournisseurs qui optimisent leurs performances afin d'avoir la meilleure note possible sur ce qui est mesuré. Les aspects du service qui ne sont pas mesurés, quelle que soit leur importance en théorie, seront délaissés à cause des pressions courantes de la prestation du service.

Les clients sont souvent attirés par l'idée que les fournisseurs devraient être tenus responsables du coût total de tout manquement aux modalités et conditions contractuelles. En cas de manquement important, le fournisseur pourrait devoir faire face à une perte garantie sur le service. À cause de modalités contractuelles strictes, il n'y a rien que la personne responsable puisse faire pour redresser la situation ou réduire la perte. Cela devient un puissant frein à la motivation. Des recours devraient être structurés de manière à ce que le fournisseur ait toujours un stimulant pour essayer encore plus fort.

Nous avons les connaissances requises pour établir des accords efficaces sur les niveaux de service TI. La BITI fournit une orientation utile. Il y a de nombreux contrats de services TI en sous-traitance[250] qui prétendent suivre le cadre BITI. En dépit de l'existence de la BITI (ITIL) et de pratiques exemplaires semblables, « une étude Gartner indique que la moitié des projets donnés en sous-traitance cette année [2003] seront étiquetés comme des « perdants » par les principaux décideurs[251] ». Il y a de nombreux facteurs qui contribuent à ce taux élevé d'échec prévu. L'un des principaux défis est que le service TI requis change, mais que nous n'avons pas de moyens efficaces pour modifier les responsabilités afin de suivre les changements du service. Nous pouvons envisager la façon dont les responsabilités en matière de services TI pourront être effectivement modifiées afin de suivre les changements dans les services TI à fournir.

10.5 Matériel

10.5.1 Définition du matériel

L'infrastructure d'information comprend les composants des systèmes informatiques et les composants des systèmes de communications. Toutes les infrastructures essentielles qui dépendent de l'infrastructure d'information essentielle (par exemple, le réseau d'électricité, le secteur des services financiers, etc.) dépendent des télécommunications, soit le réseau public de télécommunications, les réseaux par satellite et Internet ainsi que les réseaux sans fil terrestres. Les biens matériels comprennent les ordinateurs et les appareils périphériques, les routeurs, les commutateurs, etc. Les composants du matériel de communications comprennent les lignes de

[249]Deux des participants au présent document, Mark Stirling et Robert Fabian, ont une expérience pratique importante dans la prestation des services TI et avec les accords sur les niveaux de service. Les points à soulever sont tirés en grande partie de cette expérience canadienne et internationale.

[250]« Purchasing a significant percentage of intermediate components from outside suppliers. » Cette définition se trouve dans le glossaire *Campbell R. Harvey's Hypertextual Finance Glossary*, en ligne : <http://www.duke.edu/~charvey/Classes/wpg/bfgloso.htm>.

[251]Gregg Keizer, « Outsourcing: A 50-50 Proposition » *InformationWeek* (26 mars 2003), en ligne : Information Week <http://www.informationweek.com/story/IWK20030326S0006>.

transmission de divers types, constituées essentiellement des fils et des câbles traditionnels, ainsi que les lignes à fibres optiques. En outre, il y a les satellites de télécommunications et l'équipement associé des liaisons montantes et descendantes.

10.5.2 Mécanismes de responsabilité dans le domaine du matériel

10.5.2.1 Garanties et conditions implicites

Contrairement au logiciel, qui est typiquement sous licence, le matériel informatique peut être vendu définitivement et le contrat d'achat donnera à l'acheteur le titre de propriété de l'équipement. Le matériel informatique peut être également pris en location ou à bail et le contrat de location permettra à l'utilisateur de se servir de l'équipement pendant un certain temps en payant des frais périodiques.

Toutes les provinces de la common law ont des lois sur la vente de marchandises qui comprennent plusieurs garanties et conditions. Celles-ci sont généralement implicites dans tous les contrats de vente de marchandises. Toutefois, elles peuvent être expressément exclues, sauf lorsqu'il s'agit de ventes à des consommateurs[252]. Dans de tels cas (par exemple, lorsque des PC sont vendus pour un usage à domicile), la plupart des lois provinciales sur la protection des consommateurs contiennent souvent des règles spécifiques quant aux garanties des consommateurs et elles peuvent rejeter l'avis d'exclusion des garanties et conditions implicites selon les lois sur la vente d'objets[253]. Même si des ordinateurs personnels et l'équipement associé se trouvent dans l'infrastructure d'information plus vaste, pour les besoins du présent rapport, l'infrastructure d'information essentielle sera jugée ne pas inclure du matériel informatique et des produits associés achetés pour l'utilisation à domicile (pas pour les affaires). Cependant, les ordinateurs à domicile peuvent présenter le risque (non quantifié jusqu'à présent) de détournement à des fins de déni de service, de redirection pour la pénétration d'un système, d'envoi de pourriels, etc. Ainsi, même s'ils ne font pas partie de l'infrastructure d'information essentielle, les ordinateurs à domicile peuvent avoir un impact sur l'infrastructure d'information essentielle.

En ce qui concerne la vente du matériel (contrairement à celle du logiciel), il n'y a aucune confusion quant à savoir s'il s'agit ou non d'une vente d'objet. Par exemple, la *Loi sur la vente d'objets*[254] de l'Ontario contient la définition suivante d'« objets » :

> « objets » Choses, à l'exclusion des droits d'action et des sommes d'argent. La présente définition s'entend en outre des produits agricoles, des récoltes sur pied cultivées et des choses attachées à un bien-fonds ou en faisant partie intégrante, dont il est convenu qu'elles en seront séparées avant la vente ou aux termes du contrat de vente. (« goods »)

Il est assez évident qu'un élément du matériel informatique ou de l'équipement de communications connexe entre clairement dans le cadre de cette définition d'objets (*chatel personnel).* Ainsi, étant donné que la Législation sur la vente d'objets s'applique au matériel

---

[252] Note : Dans certaines juridictions, les garanties et conditions implicites contenues dans les lois sur la vente d'objets ne peuvent pas être exclues dans le cas de ventes à des « consommateurs » (c'est-à-dire des entités qui ne sont pas des entreprises).
[253]Takach, *supra* note 192 à 473.
[254]R.S.O. 1990, Chapter S.1.

envisagé, plusieurs garanties et conditions implicites s'appliqueront à la vente du matériel à moins d'une entente spécifique à cet égard. Tout d'abord, si le fournisseur est un marchand et que les objets sont achetés d'après une description donnée par le fournisseur qui fait le commerce d'objets de cette description, les produits fournis doivent alors être de « qualité marchande » (c'est-à-dire qu'ils sont appropriés aux fins prévues)[255].

La deuxième condition (et garantie) implicite importante énonce ce qui suit :

1. Lorsque l'acheteur se fie aux compétences et aux connaissances du fournisseur et que
2. le fournisseur a une connaissance précise de l'usage qui sera fait des objets dans les locaux de l'acheteur,

alors le fournisseur doit donner des objets qui sont adaptés à cet usage particulier[256].
Pour que cette deuxième condition (et garantie) implicite s'applique, le fournisseur doit être informé des exigences spécifiques de l'utilisateur. À titre d'exemple, dans l'affaire *Saskatoon Gold Brokers* c. *Datatec Computer Systems Ltd*.[257], le tribunal a jugé que le fournisseur d'un système informatique n'était pas responsable du fait que le système n'a pas rempli une fonction cruciale. En effet, le fournisseur n'avait jamais été informé de la nécessité d'une telle fonction par l'acheteur; on n'avait pas dit au fournisseur que l'aspect gestion de l'inventaire de l'entreprise comprenait une composante de fabrication, ce que le système informatique ne supportait pas.

Dans la décision de l'Ontario, *Classified Directory Publishers* c. *Image Management Technologies Inc*.[258], un fournisseur n'a pas été trouvé responsable en vertu de l'article 15(1) de la *Loi sur la vente d'objets* de l'Ontario (l'article sur la condition implicite d'adaptation à l'usage particulier de l'objet). Le fournisseur avait vendu une unité de stockage à disque optique qui n'avait pas bien fonctionné avec le matériel informatique de l'acheteur. Toutefois, l'acheteur n'avait pas informé le fournisseur quant à l'utilisation qu'il voulait faire de l'unité de disque. L'unité du fournisseur était conçue pour du stockage en ligne secondaire alors que l'acheteur voulait du stockage en ligne principal. Le tribunal a décidé que le fournisseur n'était pas responsable de cette disparité. En justifiant sa décision, le tribunal a déclaré :

> Le demandeur a choisi l'équipement du défendeur sans informer entièrement le défendeur de l'utilisation prévue, sans expertise suffisante de sa propre part et sans se fier à des consultants qui étaient disponibles à cet égard. Il n'a pas été établi que la défaillance du système peut être attribuée à l'équipement fourni par le défendeur. Il n'y a

[255]Par exemple, la *Loi sur la vente d'objets* (*Sale of Goods Act*) de l'Ontario déclare à l'article 15(2),
« Il y a une condition implicite que les objets achetés sur description sont de qualité marchande si le vendeur fait le commerce d'objets de cette description (qu'il en soit ou non le fabricant). Si l'acheteur a examiné les objets, il n'y a pas de condition implicite relative aux vices que l'examen aurait dû révéler. »

[256]Par exemple, voir l'article 15(1) de la *Loi sur la vente d'objets* (*Sale of Goods Act*) de l'Ontario qui déclare :
« Il y a une condition implicite que les objets sont raisonnablement adaptés à l'usage particulier que l'acheteur fait connaître expressément ou implicitement au vendeur, en montrant qu'il s'en remet à la compétence ou au jugement de celui-ci, lorsque les objets correspondent à la description de ceux que le vendeur fournit dans le cours de son commerce, qu'il en soit ou non le fabricant. Il n'y a pas de condition implicite relative à l'adaptation à un usage particulier d'un article déterminé sous son brevet ou sous une autre appellation commerciale. »

[257]*Saskatoon Gold Brokers* v. *Datatec Computer Systems Ltd*.. (1986), 55 Sask. R. 241 (Q.B.).

[258][1995] O.J. No. 36 (Gen. Div.).

> aucune preuve qu'il serait impossible de déterminer la raison d'une telle défaillance. Les éléments essentiels à la demande de garantie en vertu de l'article 15 n'ont donc pas été établis.

Par ailleurs, lorsque l'acheteur informe le fournisseur de l'utilisation prévue du produit et que le fournisseur indique que le produit peut répondre à ce besoin spécifique, le tribunal peut alors décider que les garanties et conditions quant à l'adaptation du produit à son usage particulier s'appliquent, comme il est indiqué dans la loi.

Les lois sur la vente d'objets comprennent un autre mécanisme de responsabilité qui peut s'appliquer au matériel. Plus précisément, ces lois tiennent compte du moment où l'acheteur est censé avoir accepté les objets de la part du fournisseur (en supposant que ce n'est pas spécifiquement indiqué dans un contrat écrit). Ce point est important car, une fois le produit accepté, l'acheteur est en général limité aux dommages pécuniaires en cas de mauvais fonctionnement ultérieur du matériel. Par contre, avant que le produit ait été jugé accepté par l'acheteur, celui-ci a le droit d'annuler la vente et de recevoir un remboursement complet[259].

10.5.2.2 Limitations de responsabilité

Même si cela se fait généralement dans le cas du logiciel, les fournisseurs de matériel peuvent parfois exclure toutes les garanties et conditions implicites dans le contrat de vente. Dans le cas du matériel, un scénario plus probable est celui où le fournisseur indique une limitation générale de sa responsabilité dans le contrat de vente. Par exemple, le fournisseur du matériel peut limiter sa responsabilité à un montant fixe en dollars dans le cas de dommages directs. D'autres dommages, comme les profits perdus ou les dommages indirects, peuvent être exclus. La raison en est que l'acheteur peut utiliser le matériel informatique pour une grande variété de tâches ou de fonctions. Quelques-unes de ces utilisations n'ont peut-être jamais été prévues par le fournisseur et d'autres utilisations peuvent présenter un degré élevé de risque.

10.5.2.3 Garanties explicites

Contrairement aux garanties qui sont implicites dans la common law ou dans une convention, les garanties explicites sont des promesses verbales ou écrites du fournisseur au sujet de ce qui aura lieu si le produit est défectueux[260]. Certains contrats de vente incluront des garanties explicites. C'est souvent prudent à la lumière de la coutume dans l'industrie informatique d'exclure les garanties et conditions implicites. Ces garanties explicites vont souvent de pair avec les dispositions sur les tests d'acceptation. Si le fournisseur ne satisfait pas aux exigences des tests d'acceptation, l'acheteur a souvent droit à réparation.

10.5.3 Matériel de transmission sans fil

Le matériel de transmission sans fil présente quelques problèmes et défis uniques de responsabilité dans le contexte plus vaste de l'infrastructure d'information essentielle. Cet équipement comprend les satellites de télécommunications et les appareils associés, le matériel qui constitue les réseaux de données sans fil (par exemple, modems sans fil, routeurs sans fil,

---

[259]Takach, *supra* note 192 à 474.

[260]Crawford, C. Merle, C. Anthony Di Benedetto and Roger J. Calantone. *New products Management*. New York: Irwin McGraw-Hill, 2000.

émetteurs de station de base, etc.) ainsi que les systèmes à relais micro-ondes (émetteurs, récepteurs et matériel associé).

Tous les dispositifs de transmission sans fil partagent un attribut majeur qui a un impact sur la responsabilité, c'est-à-dire qu'ils sont soumis à des influences incontrôlables, fréquemment imprévisibles et éventuellement néfastes. Ces « cas de force majeure » comprennent les orages et les éruptions solaires, d'autres perturbations électromagnétiques (EM) d'origine cosmique, des phénomènes météorologiques adverses extrêmes, etc. Les satellites de télécommunications eux-mêmes sont soumis à d'autres risques imprévisibles, comme les collisions avec des météores ou avec des débris spatiaux.

À cause de ces facteurs, le matériel de transmission sans fil souffre d'un manque inhérent de prévisibilité quant à la largeur de bande disponible. Il devient donc pratiquement impossible de garantir un niveau spécifié de temps de bon fonctionnement et de fiabilité. Tel n'est pas le cas pour les appareils branchés pour lesquels on peut généralement assurer (ou au moins prévoir) des niveaux spécifiques de temps de bon fonctionnement. En outre, même si on peut concevoir diverses redondances dans les systèmes câblés, ce n'est pas possible pour du matériel totalement sans fil puisqu'il sera toujours soumis aux perturbations EM mentionnées ci-dessus.

À la lumière de la croissance rapide et de l'importance de la technologie sans fil, il est essentiel que des mécanismes appropriés de responsabilité soient établis et mis en œuvre pour les appareils de transmission sans fil. Toutefois, l'examen détaillé de ces mécanismes de responsabilité est en dehors de la portée du présent rapport, mais cela pourrait faire l'objet de recherches et d'études ultérieures.

10.5.4 Normes

La capacité d'établir, de raffiner et d'appliquer les exigences en matière de responsabilité dépend de la capacité (nécessaire) de quantifier et d'évaluer les exigences en fonction d'une norme ou d'un banc d'essai. Les normes facilitent les mesures requises. Un certain nombre de normes différentes ont évolué dans le domaine de l'équipement sans fil. Elles comprennent les normes établies par l'Association canadienne de normalisation (ACNOR/CSA), Industrie Canada et Santé Canada.

Voici quelques-unes des normes de l'ACNOR (CSA) qu'il faut suivre pour le matériel de transmission sans fil :

- CAN/CSA-CEI/IEC CISPR 22-02 : Appareils de traitement de l'information – Caractéristiques des perturbations radioélectriques – Limites et méthodes de mesure
- C22.2 NO. 98-1954 (R2002) – Construction et essais des émetteurs radioélectriques
- C108.8-M1983 (R2000) – Impulsions électromagnétiques produites par les matériels de traitement de l'information et de bureautique : valeurs limites et méthodes de mesure

- C22.1 SB-02 – Code canadien de l'électricité, Première partie (19e édition), Norme de sécurité relative aux installations électriques[261]

Le matériel de transmission sans fil est également touché par les normes d'Industrie Canada, y compris le Cahier des charges révisé sur les normes radioélectriques (CNR/RSS). Un tel équipement est requis pour respecter certaines normes minimales de fréquences radio comme les limites d'émission à l'extérieur des blocs de fréquences et le seuil de tolérance de la dérive de fréquence. Comme il est énoncé dans la publication d'Industrie Canada, Gestion du spectre et Politique des télécommunications :

> « Les normes seront élaborées en consultation avec l'industrie et le Cahier des charges sur les normes radioélectriques (CNR) pertinent sera révisé en conséquence. Les fournisseurs devront certifier la conformité de leur matériel aux dispositions du CNR révisé, selon le processus d'approbation technique d'Industrie Canada[262]. »

Voici quelques-unes des normes d'Industrie Canada qui s'appliquent au matériel de transmission sans fil :

- CNR-191 (RSS) – Systèmes de télécommunications multipoints locaux dans la bande de 28 GHz et systèmes de télécommunications point à point et point à multipoints à large bande dans les bandes de 24 GHz et de 38 GHz (provisoire)
- CNR-195 – Matériel du service de communication sans fil exploité dans les bandes de 2 305–2 320 MHz et 2 345–2 360 MHz
- CNR-192 – Matériel fixe d'accès sans fil exploité dans la bande de 3 450–3 650 MHz
- CNR-210 – Dispositifs de radiocommunications de faible puissance, exempts de licence (pour toutes les bandes de fréquences)
- NMB-003 (ICES-003) – Appareils numériques (la présente norme sur le matériel brouilleur établit les exigences techniques relatives au bruit radioélectrique transmis par rayonnement et par conduction en provenance d'appareils numériques)

Finalement, le matériel de transmission sans fil est soumis aux normes de Santé Canada, comme celle sur les *Limites d'exposition humaine aux champs de radiofréquences électromagnétiques dans la gamme de fréquences de 3 kHz à 300 GHz – Code de sécurité 6*[263]. Le but de cette norme

---

[261] Association canadienne de normalisation (Canadian Standards Association), normes acceptées (2004), en ligne : Association canadienne de normalisation – pages Web Normes sur l'électricité et l'électronique et Normes sur les communications <http://www.csa.ca/standards/electrical/Default.asp?language=English> et <http://www.csa.ca/standards/communications/Default.asp?language=English>.

[262] Industrie Canada, « Politique et procédures pour la délivrance de licences par enchère dans les bandes de fréquences de 24 et 38 GHz » *Gestion du spectre et Politique des télécommunications* (29 mai 1999), en ligne : site Web Strategis d'Industrie Canada <http://strategis.ic.gc.ca/epic/internet/insmt-gst.nsf/vwapj/AUCTIONS9.PDF/$FILE/AUCTIONS9.PDF>.

[263] Santé Canada, *Limites d'exposition humaine aux champs de radiofréquences électromagnétiques dans la gamme de fréquences de 3 kHz à 300 GHz – Code de sécurité 6* (17 octobre 2002), en ligne : page Web Bureau de la protection contre les rayonnements des produits cliniques et de consommation de Santé Canada <http://www.hc-sc.gc.ca/hecs-sesc/ccrpb/publication/99ehd237/toc.htm>.

ou du Code est d’établir des exigences de sécurité pour l’installation et l’utilisation des appareils micro-ondes et radiofréquences (RF) qui fonctionnent dans la gamme de fréquences de 3 kHz à 300 GHz. Cette gamme de fréquences inclut de nombreux appareils de transmission sans fil qui font partie de l’infrastructure d’information essentielle.

11.0 État actuel de la responsabilité dans l'infrastructure d'information

En fait, cette section du rapport peut être très brève. Presque personne n'accepte la responsabilité de l'exécution du service public de bout en bout dans le cadre de l'infrastructure d'information du Canada. Les participants limitent, restreignent et circonscrivent soigneusement la responsabilité qu'ils sont prêts à accepter. Il est néanmoins vrai que nous avons un grand nombre de participants reconnus dans notre infrastructure d'information. Ils voient les dangers actuels auxquels l'infrastructure d'information du Canada doit faire face et ils ont des opinions au sujet de ce qui peut, devrait ou doit être fait pour notre infrastructure d'information essentielle.

Nous commençons par décrire les dix perceptions clés qui ont fait surface pendant nos premières entrevues avec les participants et au cours de notre étude approfondie des ouvrages auxiliaires. Cela donne une image utile de ce que les participants de l'infrastructure d'information estiment être l'état actuel et les perspectives d'avenir de cette ressource nationale clé. Cette section du rapport conclut par des éléments qui font le lien entre les préoccupations en matière de responsabilité et les approches de gouvernance qui ont été suivies traditionnellement pour l'Internet, à l'échelle nationale et internationale.

11.1 Perceptions des participants

11.1.1 Infrastructure vulnérable aux attaques

Tous les participants que nous avons interrogés estimaient qu'il y avait de bonnes raisons d'avoir des appréhensions au sujet de l'état de l'infrastructure d'information essentielle au Canada. Toutefois, les opinions variaient quelque peu. Certains participants pensaient que l'Internet, et par extension l'infrastructure d'information du Canada, n'était pas intrinsèquement sûr ni fiable. Une personne est allée même jusqu'à nous conseiller de garder notre infrastructure d'information essentielle entièrement séparée du réseau plus vaste d'Internet.

Les « optimistes » croyaient qu'il y avait des choses que le Canada pouvait faire pour améliorer la fiabilité, la disponibilité et la sécurité de notre infrastructure d'information essentielle. Cependant, même eux n'étaient pas convaincus qu'il y avait une préoccupation publique suffisamment forte pour galvaniser le Canada afin qu'il prenne des mesures à temps pour empêcher des pannes majeures dans notre infrastructure d'information essentielle.

11.1.2 Pannes probables à venir

Pratiquement toutes les personnes interrogées estimaient qu'une panne majeure de l'infrastructure d'information essentielle du Canada était probable… *dans les cinq prochaines années!* Cet avis, plus que toute autre observation faite à la suite de notre recherche primaire (et secondaire), doit nous préoccuper beaucoup. Les problèmes sont reconnus partout. Il y a des voies reconnues que le Canada (et d'autres pays) devaient suivre afin de réduire les risques pour notre infrastructure d'information essentielle. Mais aucune des personnes interrogées ne croyait que nous allions agir à temps pour prévenir une panne majeure dans les cinq prochaines années.

Est-ce que cette panne future sera suffisante pour galvaniser le Canada et le monde et les pousser à agir? Si ce n'est pas la première panne majeure, alors l'une des pannes suivantes peut nous pousser à suivre un plan d'action collectif. Le défi à court terme consiste à déterminer les mesures que nous devrions prendre lorsque nous aurons la volonté d'agir. Le danger, c'est de se

retrouver dans une situation où il faut absolument agir, mais pour laquelle le terrain n'a pas été bien préparé. Nous pouvons nous retrouver forcés de prendre des mesures inappropriées.

11.1.3 Pannes antérieures

Plusieurs observateurs ont déclaré que la mégapanne d'électricité de 2003 avait été causée (en partie) par la panne d'un composant clé de l'infrastructure d'information de l'Amérique du Nord. Il y a un cas documenté du ver Slammer qui a neutralisé un système de surveillance de la sécurité dans un réacteur de la centrale nucléaire Davis-Besse, en Ohio, pendant une période de cinq heures en janvier 2003[264]. Heureusement, le réacteur touché était arrêté au moment où cela s'est produit, mais *cela s'est* produit. Et c'est vrai aussi que le ver Blaster était tout juste en train de se répandre lorsque la panne d'électricité s'est produite[265]. Est-ce que le ver Blaster a pu neutraliser un système de surveillance critique tout juste au bon (mauvais) moment? Peut-être.

Nous ne prétendons pas que le ver Blaster a provoqué la mégapanne d'électricité de 2003. Le point intéressant est que plusieurs informateurs éclairés sont prêts à croire que ce ver aurait pu être un facteur causal important. Cela renforce les observations au sujet des risques et des pannes probables à venir dans notre infrastructure d'information essentielle.

11.1.4 Problèmes de monopole

Un tribunal des États-Unis a jugé que Microsoft était un monopole[266]. Une argumentation puissante a été montée selon laquelle la monoculture résultante de Microsoft représente une menace sérieuse pour la sécurité cybernétique[267]. C'est un argument par analogie. Les monocultures en agriculture sont connues pour être particulièrement vulnérables aux attaques[268] et particulièrement incapables de se défendre contre ces attaques. On se préoccupe donc du fait que notre monoculture de bureau Microsoft pose une menace semblable à la cyber-sécurité.

Plusieurs personnes interrogées ont déclaré que la monoculture de monopole de Microsoft était un danger. Même si l'analogie agricole n'est pas acceptée et que cet argument n'est pas admis

---

[264]Voir Duncan Graham-Rowe, « Electricity grids left wide open to hackers » *New Scientist Online News* (27 août 2003), en ligne : New Scientist.com <http://www.newscientist.com/hottopics/tech/article.jsp?id=99994094&sub=Transport%20and%20Energy>.

[265]Voir Kayla Michaels, « Blackout 2003: Could have Been Internet Worm/Virus; Bush Blocked Funding to Protect the Grid » *OpEdNews.com* (15 août 2003), en ligne : OpEdNews <http://www.opednews.com/michaels_blackout_2003.htm>.

[266] L'une des décisions dans l'affaire récente aux États-Unis contre Microsoft a été de déterminer que Microsoft était un monopole. Voir BBC News Staff, « Microsoft vs U.S. Justice Dept » *BBC News* (23 novembre 1999), en ligne : BBC News World Edition <http://news.bbc.co.uk/1/hi/special_report/1998/04/98/microsoft/201889.stm>.

[267]Geer *et al.*, *supra* note 63.

[268]« La variété la plus courante de banane, qui a été cultivée pour en faire un fruit sans graines jusqu'au point de la rendre infertile, subit de 40 à 50 % de pertes chaque année à cause des insectes nuisibles. Et 85 % des orangers au Brésil, qui est le premier producteur au monde d'oranges, sont sensibles à un mystérieux fléau appelé « *mort soudaine* ». Voir Robert Lemos, « Agriculture epidemics may hold clues to Net viruses » *ZD Net Australia* (16 janvier 2004), en ligne : ZD Net Australia <http://www.zdnet.com.au/news/security/0,2000061744,39115682,00.htm>.

par tous[269], il y a encore un certain nombre de dangers dans un marché de monopole. Aucun fournisseur qui occupe une position de monopole ne peut apporter sans réfléchir des changements à ses produits; trop de choses dépendent des « fonctions » que d'autres estiment qu'il faut corriger. Nous n'offrons aucune conclusion au sujet de Microsoft et des monocultures, mais nous signalons que le quasi-monopole de Microsoft dans le bureau et dans le marché des suites bureautiques peut nécessiter des réponses particulières.

11.1.5 Portée internationale

Notre recherche primaire et secondaire a toujours mené à la conclusion que l'infrastructure d'information essentielle au Canada ne peut pas être véritablement séparée de l'infrastructure d'information mondiale. Nous ne sommes pas et ne pourrons jamais être une île, bien à l'abri tout seuls dans le cyberespace. Le monde en dehors de nos frontières aura un impact profond sur ce que nous pouvons, devrions et devrons faire au sujet de notre infrastructure d'information essentielle.

L'une des personnes interrogées a signalé toutefois que cette interdépendance pourrait permettre au Canada de jouer un rôle de premier plan. Nous pourrions aider le monde à découvrir de meilleures façons de réaliser une infrastructure d'information essentielle fiable, accessible et sûre. Outre la fierté justifiable que le Canada pourrait tirer d'un tel rôle de leadership, cela pourrait également offrir aux fournisseurs canadiens des débouchés commerciaux importants pour ce qui est d'aider d'autres pays avec leur infrastructure d'information essentielle.

11.1.6 Normes professionnelles

Les professions traditionnelles comme la médecine et la comptabilité ont établi des normes de pratique que doivent suivre tous les praticiens agréés. Il y a un grand nombre, toujours croissant, de normes proposées dans le domaine de la sécurité informatique et des réseaux[270]. Il existe plusieurs programmes de certification pour les professionnels de la sécurité en informatique[271]. Plusieurs personnes interrogées ont exprimé le souhait que les responsables de notre infrastructure d'information essentielle soient tenus de suivre le même genre de normes de pratique que les professionnels traditionnels.

La certification peut aider, mais il n'y a aucune force de loi derrière la certification volontaire et tous les efforts de certification en matière de sécurité ont été jusqu'à présent des efforts volontaires. Contrairement à la plupart de nos partenaires commerciaux, le Canada a des secteurs de pratique réservés ou restreints qui sont prévus dans les lois provinciales autorisant les sociétés

---

[269]Voir Mike Gunderloy, « Questioning the Monoculture Argument » *ADTMAG.com* (19 janvier 2004), en ligne : Application Development Trends Magazine <http://www.adtmag.com/print.asp?id=8793>.

[270]La série de normes de sécurité est étendue. L'ISO 17799 est traitée ailleurs dans ce rapport. Ici, nous voudrions seulement signaler la norme COBIT (<http://www.isaca.org/>), la norme sur la sécurité de l'information (Standard for Information Security) (<www.isfsecuritystandard.com>) et les lignes directrices sur le contrôle des technologies de l'information (Information Technology Control Guidelines) des comptables agréés du Canada (<http://www.cica.ca/index.cfm/ci_id/1004/la_id/1.htm>).

[271]L'International Information Systems Security Certification Consortium est l'un des organismes internationaux qui fournit une telle certification. Voir en ligne : <https://www.isc2.org/cgi-bin/index.cgi>.

ou les ordres professionnels de génie[272]. Il serait certainement possible d'imaginer un avenir au Canada dans lequel un permis approprié de génie serait requis afin d'exercer dans le domaine de la sécurité informatique et de réseau. Une telle décision pourrait, presque certainement, engendrer une opposition considérable[273].

11.1.7 Scepticisme du gouvernement

Toute l'histoire de l'Internet a été celle d'une réglementation minimale. Les gouvernements n'ont pas eu beaucoup de succès lorsqu'ils ont essayé de faire autre chose que de financer de nouveaux développements ou de la recherche pour des développements possibles à plus long terme. C'était presque une façon de dire : « Donnez-nous l'argent, mais ne nous ennuyez pas avec vos conditions abusives. » Et, somme toute, l'Internet a incroyablement réussi.

Bien des gens qui nous ont parlé ont exprimé un profond scepticisme au sujet des interventions des gouvernements. Ce que nous voulons souligner, ce n'est pas le fait que le gouvernement ne peut pas ou ne devrait pas réglementer, mais plutôt qu'il devrait reconnaître que de nombreux participants voient la réglementation du gouvernement comme quelque chose à laquelle il faudrait automatiquement s'opposer. Au minimum, il faut tenir compte de cette perception répandue lorsqu'il s'agit d'établir des plans pour introduire une réglementation publique.

11.1.8 Financement nécessaire

Tout comme les participants sont prêts à s'opposer à la réglementation gouvernementale, ils sont aussi prêts à reconnaître l'importance du financement du gouvernement dans les initiatives de collaboration et les projets. Comme il est décrit ailleurs dans ce rapport, l'Internet a eu pour origine des projets financés par le Department of Defence des États-Unis. Et, pendant de nombreuses années, le service de base d'Internet a été fortement subventionné par le gouvernement américain. Tout le monde reconnaît que le financement public approprié de projets peut donner lieu à des améliorations importantes et utiles dans notre infrastructure d'information. Notre propre Réseau canadien pour l'avancement de la recherche, de l'industrie et de l'enseignement (CANARIE)[274] est un exemple respecté de la façon dont les fonds publics peuvent être appréciés par nos participants de l'Internet. Des modèles de financement semblables pourraient être envisagés en relation avec l'infrastructure d'information essentielle du Canada.

---

[272]L'explication sur la façon dont cela fonctionne en Alberta et en Ontario se trouve dans les sites Web APEGGA et PEO; voir en ligne : <http://www.apegga.org> et <http://www.peo.on.ca>.

[273]La Société canadienne de traitement de l'information a protesté contre les décisions de divers organismes de génie au Canada de réserver le droit au titre d'ingénieurs logiciels. Voir en ligne : <http://www.cips.ca/it/position/software/>. On peut s'attendre à une opposition semblable dans le cas de décisions visant à restreindre le droit au titre, ou le droit à la pratique, dans les domaines de la sécurité informatique ou de réseau.

[274]« Canarie Inc. – le fer de lance de l'Internet évolué au Canada – est un organisme sans but lucratif soutenu par ses membres, par ses partenaires de projet et par le gouvernement fédéral. » Voir en ligne : <http://www.canarie.ca/about/about.html>.

11.1.9 Attention requise

L'argent public peut aider, mais ce qui est encore plus important, c'est la reconnaissance publique que le Canada fait face à un certain nombre de défis importants en relation avec notre infrastructure d'information essentielle. Le public est heureux de jouir des bienfaits d'une circulation rapide et transparente des données qui est rendue possible par notre infrastructure d'information. Mais c'est une capacité qui est largement invisible pour le grand public. En général, le public ne sait pas ou ne tient pas à savoir quel est le rôle mobilisateur de notre infrastructure d'information. Et le public ne reconnaît certainement pas l'importance des mesures qui visent à améliorer la fiabilité, l'accessibilité et la sécurité de notre infrastructure d'information essentielle. Les personnes que nous avons interrogées ont toutes reconnu que ce point est important lorsqu'il s'agit d'établir des plans pour notre infrastructure d'information essentielle.

11.1.10 Force externe

Le dernier point de notre liste fait suite à des réflexions sur les raisons de notre succès de l'An 2000 puisque les mesures correctives ont eu pour résultat un nombre très peu important de pannes. Dans une grande mesure, les personnes qui étaient directement responsables des systèmes d'information ne pouvaient pas obtenir le soutien complet des cadres supérieurs pour leurs mesures correctives de l'An 2000. Des ressources ont été consacrées aux mesures correctives de l'An 2000 *après* que des participants externes importants ont commencé à insister sur l'importance de ces mesures. Des banquiers, des comptables ou des avocats ont conseillé à leurs clients ou ont insisté auprès d'eux pour qu'ils fassent attention aux problèmes éventuels de l'An 2000. Il semblait que tout le monde se préoccupait de l'An 2000.

Ce genre de force externe massive a été suffisant pour « résoudre » le problème de l'An 2000[275]. Ce serait souhaitable de pouvoir éviter la nécessité d'une telle force externe massive comme motivation pour relever le défi de l'infrastructure d'information essentielle. Tout d'abord, nous aurions comme résultat probable un processus très inefficace et qui serait assez coûteux. En second lieu, cette force ne s'applique en général qu'à la suite d'une panne importante qui sensibilise au plus haut point le public : ce serait bien si nous pouvions éviter ce genre de panne sérieuse.

[275]Étant donné l'énorme pression qui a été appliquée, il n'est pas surprenant de voir l'inefficacité assez considérable avec laquelle les organisations ont abordé leurs problèmes An 2000. Dans un monde parfait, un tout petit peu moins de pression aurait pu donner une plus grande efficacité, mais beaucoup moins de pression aurait pu nous laisser avec des problèmes majeurs de l'An 2000.

11.2 État de la responsabilité

À ses débuts, l'Internet a été surtout lancé pour le partage d'égal à égal de ressources entre différents réseaux. Cela contrastait vivement avec les modèles de contrôle centralisés qui étaient alors courants dans les autres réseaux informatiques[276]. Il n'y avait aucune autorité centrale de l'Internet. Bien entendu, l'argent fédéral américain a aidé à sa réalisation, mais un bon nombre des principaux rôles étaient remplis sur une base volontaire par des membres intéressés de la communauté Internet[277]. Cette approche de partage volontaire a coloré toutes les premières idées au sujet de l'Internet et de la façon dont le réseau devrait être gouverné. La responsabilité en vertu de la loi était très loin des premières préoccupations au sujet de l'Internet.

Les étudiants en droit de l'Université Harvard ont fait un résumé intéressant de la gouvernance Internet en 2000. Dans l'introduction de leur article collectif à ce sujet, ils posent une question de base sur ce qui est requis par l'Internet :

> Étant donné que l'Internet a rempli sa promesse, toujours plus reconnue, de devenir un élément de transformation culturel, économique et politique, une attention croissante a été accordée à la question de savoir si nous avons besoin d'une gouvernance de l'Internet et, si tel est le cas, sous quelle forme. Avons-nous besoin d'une structure formelle de gouvernance ou est-ce qu'un moyen informel de gouvernance suffira, c'est-à-dire des normes de comportement établies par la communauté Internet ou par le code lui-même[278]?

Les normes de la communauté Internet ont servi véritablement à mettre en vigueur les normes[279] requises pour l'interconnexion des réseaux et, si un participant viole constamment ces normes, l'accès à d'autres réseaux lui sera refusé. Le processus a fait ses preuves et il a eu un succès remarquable.

---

[276]L'architecture unifiée de réseau SNA (System Network Architecture) d'IBM était alors l'une des principales architectures de réseau. Elle avait un gros ordinateur d'IBM comme noyau logique. « Il s'agit d'un protocole de réseau à sept couches. Chaque couche du protocole a un ensemble de services de transmission de données associés. Les services de la couche supérieure sont intégrés en une unité logique. Chaque type d'unité logique défini dans l'architecture a son propre ensemble spécifique de services offerts à un utilisateur final pour la communication. l'utilisateur final peut être un appareil terminal ou un programme d'application. La structure SNA permet à l'utilisateur final de fonctionner indépendamment, sans être touché par les fonctions précises utilisées pour l'échange de l'information. » Voir en ligne : <http://edocs.bea.com/elink/elinkjam/v411/jamug/gloss.htm>.

[277]Pendant de nombreuses années, l'Université de la Colombie-Britannique a pris en charge l'attribution des domaines canadiens sur une base volontaire. Personne n'a payé l'Université pour faire ce travail. C'était sa contribution au bien collectif canadien. Voir *A Nation Goes ONLINE*, CA.net Institute, en ligne : <http://www.canarie.ca/press/publications/ango.pdf>.

[278]Gina Paik & P-R Stark, « The Debate Over Internet Governance: A Snapshot in the Year 2000 », en ligne : The Berkman Center for Internet & Society at Harvard Law School <http://cyber.law.harvard.edu/is99/governance/introduction.html>.

[279]La plupart des normes Internet ont commencé comme des documents RFC (Request For Comment). Il y avait consensus, ou non, sur la proposition mise de l'avant par la demande de commentaires RFC. Le processus a commencé en 1969 avec la RFC 1 – voir <http://www.rfc-archive.org/getrfc?rfc=1>. Il a progressé au point que la RFC la plus récente portait le numéro 3729 et était datée de mars 2004 – voir <http://www.rfc-archive.org/getrfc?rfc=3729>. Les documents RFC sont maintenant supervisés par la Société Internet – voir <http://www.isoc.org/isoc/>.

Le point essentiel, c'est d'avoir une autorité centrale. Il ne doit y avoir qu'un seul et unique système pour traduire les adresses Internet que les personnes peuvent comprendre en quatre nombres entiers qui constituent les adresses réelles cybernétiques[280]. La Société pour l'attribution des noms de domaine et numéros sur Internet ICANN[281] (Internet Corporation for Assigned Names and Numbers) a été mandatée à cet égard par le gouvernement américain. La société ICANN a été fondée en 1998 et c'est un organisme sans but lucratif enregistré dans l'État de Californie. À son tour, ICANN a attribué des rôles techniques importants à la compagnie privée VeriSign[282]. Au Canada, l'Agence canadienne d'enregistrement Internet (ACEI/CIRA)[283] supervise le domaine général .ca.

ICANN a été au centre d'un certain nombre de différends continus au sujet de la façon dont Internet devrait être gouverné. En février 2004, huit registraires ont poursuivi[284] à la fois ICANN et VeriSign car ils s'estimaient désavantagés par un plan proposé par VeriSign sur les commandes en souffrance des adresses Web. VeriSign a poursuivi[285] ICANN car la compagnie veut adopter un nouveau plan à but lucratif pour rediriger les adresses Web non résolues. Et People for Internet Responsibility[286] a convoqué une réunion d'urgence sur le thème « Preventing the Internet Meltdown » pour empêcher la dissolution de l'Internet, et ce, avec le soutien vigoureux de trois personnes très versées dans le domaine[287]. Les gens se sont fort peu entendus même au sujet du rôle modeste joué par l'ICANN.

Il y a un manque presque total d'acceptation de la responsabilité dans le cas d'un service Internet partagé ou public de bout en bout. On s'attend maintenant à ce que les principaux fournisseurs du réseau de base fassent tout leur possible pour assurer le service Internet. Le système fonctionne remarquablement bien[288]. Mais on s'attend fort peu à ce que le service se poursuive « en cas de force majeure »[289]. En fait, de nombreux accords sur les niveaux de service exonèrent

---

[280]Toutes les adresses Internet se composent en fait de quatre nombres entiers, de 0 à 256. Par exemple, <www.gowlings.com> n'est véritablement que 199.43.129.10. Il est clair qu'il ne peut y avoir qu'une seule autorité pour octroyer les noms de domaine et qu'un seul mécanisme pour déterminer les véritables adresses Internet.
[281]Voir en ligne : <http://www.icann.org/>.
[282]Voir en ligne : <http://www.verisign.com/>.
[283]Voir en ligne <http://www.cira.ca/>.
[284]Matt Hicks, « Registrars Sue ICANN, VeriSign to Block Domain Name Service » *EWeek-Enterprise News and Reviews* (27 février 2004), en ligne : eWeek <http://www.eweek.com/print_article/0,1761,a=120522,00.asp>.
[285]Matt Hicks, « VeriSign Sues ICANN » *EWeek-Enterprise News and Reviews* (26 février 2004), en ligne : eWeek <http://www.eweek.com/article2/0,1759,1539737,00.asp>.
[286]Voir en ligne : PFIR - People For Internet Responsibility <http://www.pfir.org/>.
[287]Lauren Weinstein, Peter G. Neumann et David J. Farber.
[288]L'expérience personnelle des auteurs est typique. Il y a dix ans, lorsque l'Internet a été utilisé pour la première fois à des fins commerciales au Canada, toutes les connexions de l'utilisateur final étaient lentes et peu fiables. Aujourd'hui, on s'attend à ce que les principaux fournisseurs de services Internet assurent l'accès fiable au réseau à tout moment. Le service fourni aura souvent un taux d'accessibilité supérieur à 99,9 %, sans aucune perte de courriels.
[289]« Catastrophe naturelle que personne ne peut empêcher comme un tremblement de terre, un raz de marée, une éruption volcanique, un ouragan ou une tornade. Les cas de force majeure (actes de Dieu) sont importants pour deux raisons 1) pour les ravages et les dommages qu'ils provoquent et 2) parce que les contrats stipulent souvent que les « cas de force majeure » sont une excuse pour retarder ou ne pas remplir un engagement ou encore pour ne pas finir un projet de construction. De nombreuses polices d'assurance ne couvrent pas les dommages causés par des « actes de Dieu », ce qui est l'une des rares fois où une compagnie d'assurance invoque la religion. Parfois, des différends sont soulevés par la question de savoir si un orage violent ou une autre catastrophe est un cas de force majeure (et

les fournisseurs de leurs obligations contractuelles courantes lorsqu'ils sont confrontés à un « cas de force majeure ». Cependant, c'est exactement à ce moment-là que nous devrions nous préoccuper le plus de la préservation de notre infrastructure d'information essentielle.

La conclusion simple, mais inévitable, est qu'il y a très peu d'acceptation de la responsabilité pour les services partagés ou publics de bout en bout de l'infrastructure d'information au Canada. Pour établir les responsabilités, il faudrait surmonter l'obstacle des idées bien ancrées contre la réglementation qui sous-tendent l'Internet et notre infrastructure d'information. La voie de l'avenir sera pleine de défis.

---

par conséquent non couvert) ou un événement naturel prévisible. » Voir Gerald & Kathleen Hill, *Law.com Dictionary*, *s. v.* « act of God », en ligne : law.com Law Dictionary <http://dictionary.law.com/definition2.asp?selected=2318&bold=%7C%7C%7C%7C>.

12.0 Obstacles à la responsabilité

Un certain nombre de facteurs techniques, économiques, juridiques et historiques se combinent pour créer certains obstacles à la responsabilité dans les éléments de l'infrastructure d'information.

12.1 Responsabilité diluée

Comme nous l'avons mentionné ailleurs, les systèmes sont devenus de plus en plus complexes. Paradoxalement, cela s'est produit en réponse à la demande du public qui voulait avoir des systèmes plus simples à utiliser. Votre voiture n'a plus besoin d'une manivelle à l'avant et vous n'avez plus besoin de régler manuellement le point d'avance à l'allumage ni de tirer le volet de départ pour la faire démarrer[290]. Au contraire, grâce à des mécanismes complexes qui ne peuvent être réparés que par un concessionnaire, il vous suffit de tourner la clé et de partir – les systèmes sur lesquels vous comptez sont plus complexes afin de les rendre plus simples à utiliser.

Les infrastructures d'information complexes peuvent contenir des milliers d'éléments qui fonctionnent entre eux. Il n'y a pas un seul ingénieur, pas même un petit groupe d'ingénieurs, qui puisse concevoir, créer et comprendre tous ces éléments à la fois ainsi que la façon dont ils fonctionnent ensemble. Ce sont plutôt beaucoup de personnes et beaucoup de groupes qui participent à la conception des éléments. Certains les créent et d'autres encore, travaillant indépendamment, les réunissent tous en un seul système. Ceux qui en assurent la maintenance représentent encore un autre groupe d'acteurs et aucun de ceux-là, individuellement ou ensemble, ne comprend le système dans son intégralité.

Qui donc faut-il blâmer lorsque quelque chose ne va pas?

Considérons un système relativement simple comme le téléphone à domicile. Si vous achetez l'équipement d'une compagnie et que vous obtenez le service d'une autre compagnie (un scénario courant), vous pourriez vous retrouver, en cas de réparation, avec chacun des fournisseurs qui blâme l'autre lorsque le système ne fonctionne pas. Ce n'est pas le désir de décliner toute responsabilité qui provoque une telle réponse; il est beaucoup plus probable que chacun de ceux qui contribuent au système croit honnêtement que le problème n'est pas dû à son équipement ou à son service. Plus encore, cela pourrait être vrai. Le problème pourrait être dû à l'intervention d'une tierce partie, comme celle d'une pelle mécanique dans la rue en dehors de votre maison.

Par conséquent, un obstacle important lorsqu'il s'agit de tenir responsables les participants à notre infrastructure d'information organique de grande envergure peut être l'incapacité légitime de désigner un élément particulier comme la cause principale du problème. Le concept de responsabilité exige un genre quelconque de faute. Si la faute ne peut pas être imputée à un

[290]Les lecteurs plus jeunes n'auront aucune idée de ce dont nous parlons. Cela prouve le point.

participant, ou à un groupe distinct, il peut alors être difficile ou impossible d'avoir un régime de responsabilité juste et équitable[291].

12.2 Coût de la responsabilité

Le présent ouvrage a démontré plus tôt que les instruments juridiques (particulièrement les contrats de licence du logiciel) qui sont utilisés par de nombreux acteurs dans notre infrastructure d'information contiennent invariablement un langage disculpatoire qui amoindrit le coût de la faute dans les mains de ces acteurs. C'est un virage important qui transfère les risques commerciaux et financiers du fournisseur à l'utilisateur. Si la société veut maintenant tenir ces acteurs responsables au-delà des limites de ce langage disculpatoire (si les risques leur sont réattribués), ils devront alors augmenter les prix de ce qu'ils fournissent.

Le résultat, c'est que le public paiera en général plus aux fournisseurs qui ont réussi à leur soutirer les prix les plus élevés au lieu de payer davantage pour le coût d'option en cas de défaillances de l'infrastructure[292].

En bref, l'inévitabilité de coûts accrus qui doivent être assumés par ceux que la société veut tenir responsables des défaillances de notre infrastructure d'information est également un obstacle à la responsabilité.

Même s'il est incontestable que la société paie maintenant pour les défaillances périodiques de son infrastructure d'information en options perdues, il y aura un type différent de coût sociétal dans le fait de tenir responsables les fournisseurs de cette infrastructure. La responsabilité est inutile si elle n'est pas mise à exécution. Et cette mise à exécution coûte de l'argent (comprendre « des taxes »). Les législateurs devront exercer une volonté politique prodigieuse s'ils doivent à la fois tenir ces fournisseurs responsables et dépenser l'argent des contribuables pour mettre à exécution cette responsabilité[293]. La volonté politique est-elle là? S'exercera-t-elle?

Par conséquent, le coût de la mise à exécution, par action publique ou action privée, est un obstacle à une responsabilité effective.

12.3 Réduction du rythme d'innovation

Quel comportement serait stimulé par une responsabilité accrue dans le secteur de l'infrastructure d'information? Tout d'abord, les risques financiers et commerciaux accrus dus à l'imposition de la responsabilité auraient pour résultat une diffusion plus lente de produits innovateurs. La raison en est que chaque produit intégré à notre infrastructure d'information créerait une plus grande vulnérabilité pour son innovateur. Les innovateurs y penseront à deux

[291]Au cours de la panne d'électricité d'août 2003, on aurait pu pardonner à celui qui est arrivé à la conclusion que deux maximes peuvent s'appliquer : (i) « À plusieurs mains l'ouvrage avance » et (ii) « À plusieurs mains la lumière s'en va ».

[292]Les fournisseurs qui ne peuvent pas obtenir ces prix plus élevés paieront, bien entendu, leur tribut à la nature et disparaîtront.

[293]Le simple fait de donner aux membres du public un droit privé d'action, même en ces jours de popularité croissante des recours collectifs, peut être une mise à exécution insuffisante.

fois avant de lancer de nouveaux produits. Pour tempérer la réticence à introduire de nouveaux produits, il y aura le désir concurrentiel de mettre de nouveaux produits sur le marché, du moins ceux qui fonctionnent bien.

Par conséquent, le potentiel de réduction en innovation – ce que le marché n'aimera pas – constitue un obstacle possible à la responsabilité.

12.4 Concurrence

La société canadienne fait grand cas de la concurrence. La *Loi sur la concurrence* a été promulguée dans le but d'encourager la concurrence et de décourager les agissements anticoncurrentiels, y compris en particulier, la collusion dans les prix.

Il est tout à fait certain que le fait d'imposer la responsabilité aux fournisseurs de l'infrastructure d'information aura pour résultat de faire sortir quelques acteurs du marché. Les plus forts parmi ces acteurs survivront et ce sont eux qui fourniront les produits et services de notre infrastructure d'information. Le fait d'avoir moins d'acteurs dans le domaine, la responsabilité agissant comme un obstacle à l'entrée de nouveaux acteurs, pourrait bien amoindrir la concurrence et mettre une pression à la hausse sur les prix. Cela peut également agir comme une force contraire à l'encouragement de la diversité.

Nous pensons que le potentiel de retombées politiques à cause d'une concurrence réduite, ou même la perception que tel est le cas, pourrait diminuer la volonté politique d'imposer la responsabilité et donc agir comme un obstacle à la responsabilité.

12.5 Action unilatérale

Le Canada jouit d'un niveau élevé de participation dans l'infrastructure d'information mondiale. Toutefois, il n'y a pas d'hégémonie canadienne. Par conséquent, la perception selon laquelle le Canada prend des mesures unilatérales pour influer sur le régime de responsabilité pourrait agir comme un obstacle à son imposition.

Par exemple, si le Canada, agissant tout seul[294], devait édicter des lois stipulant que les limitations de responsabilité, les exclusions des garanties implicites et le langage disculpatoire dans les licences et les contrats d'acquisition n'étaient pas valables, les développeurs réagiraient en essayant de se mettre hors de portée des lois canadiennes. Les développeurs canadiens pourraient envisager de quitter le Canada et les développeurs étrangers éviteraient d'avoir un établissement permanent au Canada afin de s'assurer que la loi qui s'applique à leurs contrats serait interprétée par des tribunaux où les limitations de responsabilité, les exclusions et le langage disculpatoire seraient acceptés[295]. L'anticipation de cette réaction de la part des

[294]Cet exposé n'effleure même pas la question de savoir s'il est constitutionnel pour le gouvernement fédéral de prendre des mesures unilatérales sans l'accord des gouvernements provinciaux. Pour les fins de cet exposé, supposons qu'il existe une entière collaboration et une volonté politique au Canada à ce sujet.

[295]Il est intéressant de revoir l'affaire jugée par la Cour suprême du Canada *Morguard Investments Ltd.* v. *De Savoye*, [1990] 3 S.C.R. 1077. La cour a décidé que s'il y a un « lien réel et substantiel » entre une cause d'action et une juridiction étrangère, la décision d'un tribunal de cette juridiction étrangère doit être maintenue au Canada. Le

développeurs empêcherait le Canada de promulguer des lois qui encouragent la responsabilité et nous croyons que le Canada ne promulguerait de telles lois que de concert avec d'autres pays afin d'établir un système quasi mondial de responsabilité.

12.6 Normes

L'état actuel des normes de pratique et des normes de mesure agit comme un obstacle à la responsabilité dans le domaine de l'infrastructure d'information. Même s'il existe des normes méthodologiques[296], il faut encore établir de nombreuses normes additionnelles.

En voici la raison : afin de tenir quelqu'un responsable, il doit y avoir une mesure selon laquelle on peut déterminer si cette personne se conforme ou non aux règlements établis. La responsabilité implique l'impartialité objective dans l'application des normes, mais aujourd'hui, il n'y a aucun organisme de normalisation qui peut servir complètement de mesure de performances ou, au contraire, de mesure de la négligence dans le domaine de l'infrastructure d'information.

En d'autres termes, avant que la société puisse tenir responsables les acteurs dans le domaine de l'infrastructure d'information, les normes doivent être généralement acceptées et adoptées. Nous sommes encore très loin du compte.

12.7 Nature humaine

La nature humaine est l'un des obstacles les plus importants à la responsabilité. Nous sommes « programmés », et nous l'avons depuis l'aube de l'humanité, pour considérer les urgences comme des choses qui arrivent rapidement et non pas lentement. C'est pourquoi nous pouvons fumer pendant des décennies et ne pas considérer cela comme une urgence jusqu'à ce qu'il y ait un diagnostic de cancer. Ou encore c'est pourquoi des villages entiers peuvent être bâtis à côté d'un volcan et les habitants ne les considèrent pas comme des endroits dangereux jusqu'à ce que des flots de lave emportent tout sur leur passage. Nous sommes plus susceptibles génétiquement de considérer la charge d'un tigre comme une menace[297].

Nous sommes convaincus qu'une urgence soudaine qui provoque une perturbation majeure et durable dans notre économie est le genre d'événement qui est nécessaire pour que le public exige que les acteurs de l'infrastructure d'information soient tenus responsables du fonctionnement de leurs technologies.

---

juge LaForest a déclaré : « … les règles du droit international privé sont fondées sur la nécessité qu'impose l'époque moderne de faciliter la circulation ordonnée et équitable des richesses, des techniques et des personnes d'un pays à l'autre … Il me semble qu'en adoptant l'approche qui permet de poursuivre à l'endroit qui a un lien réel et substantiel avec l'action, on établit un équilibre raisonnable entre les droits des parties. Cela fournit une certaine protection contre le danger d'être poursuivi dans des ressorts qui n'ont que peu ou pas de lien avec l'opération ou les parties. » Par inférence, les compagnies essaient alors de réduire la possibilité que leurs activités et leurs affaires aient un « lien réel et substantiel » avec le Canada afin de rester hors de portée de la loi canadienne.

[296] Par exemple, BITI (ITIL) et ISO 17799.

[297] Même si, admettons-le, les deux sont moins menaçants dernièrement.

12.8 Usage dans le métier

Les affaires marchent le mieux dans des conditions de prévisibilité. Ce que l'on appelle l'« usage dans le métier » a été tenu pendant de nombreuses années par les tribunaux de nombreuses juridictions comme un facteur important dans l'interprétation des contrats. Lorsqu'un contrat n'est pas tout à fait clair, les tribunaux entendent souvent des arguments sur ce qui est la coutume dans le métier en particulier afin de clarifier les modalités contractuelles.

La coutume dans le métier des technologies de l'information est que les limitations de responsabilité, les exclusions dans le cas des garanties implicites et le langage disculpatoire sont utilisés dans les licences et dans les contrats d'acquisition. Même si un avocat peut consacrer beaucoup d'énergie à essayer de faire bouger l'autre partie sur l'une de ces dispositions clés, « l'usage dans le métier » prévaut le plus souvent. La nécessité de changer la culture dans le domaine des technologies de l'information est un obstacle important à la responsabilité à cause des allégations qui seront faites suivant lesquelles un tel changement est « mauvais pour les affaires ».

12.9 Compréhension incomplète

Selon le point de vue, notre infrastructure d'information est soit le montre de Frankenstein soit une merveille[298]. Une chose est vraie. Cette infrastructure est extrêmement complexe et au-delà de la compréhension d'une seule personne. Plus encore, elle évolue constamment. Sa complexité même et le fait qu'elle soit incompréhensible constituent un obstacle considérable à la responsabilité.

Pour que la société applique le concept de responsabilité dans notre infrastructure d'information, il serait bon de considérer quelle est l'approche en matière de responsabilité qui pourrait établir le meilleur équilibre entre les droits des fournisseurs du système et les droits de ses utilisateurs. Pour cela, nous devrions tout d'abord en arriver à une entente universelle sur ce que sont les droits idéaux des fournisseurs d'un côté et des utilisateurs de l'autre. Il faut ensuite s'entendre sur l'équilibre entre les deux. Finalement, nous devons convenir des étapes à suivre pour atteindre véritablement cet équilibre.

Le problème est le suivant : aucun de ces éléments n'est possible tant et aussi longtemps que nous n'avons pas une compréhension plus approfondie de la nature organique et de l'utilisation ainsi que de l'importance sociétale de notre infrastructure d'information. Si la société essaie d'imposer d'un seul coup la responsabilité complète, sans tenir compte de ces facteurs, nous ne serons pas en mesure d'extrapoler, sauf de la façon la plus rudimentaire, sur les effets que les différents modèles de responsabilité auront sur la société dans son ensemble. En bref, nous pourrions tomber de Charybde en Scylla.

[298]L'analogie est appropriée. L'infortuné monstre de Victor Frankenstein a été créé plein d'amour pour l'humanité, mais il est devenu diabolique à cause de forces qu'il ne pouvait absolument pas influencer. À la fin, le monstre a attaqué non pas son créateur, mais ceux que son créateur aimait, afin d'infliger une plus grande souffrance à son créateur.

13.0 Introduction aux modèles de responsabilité

L'état final voulu est que l'infrastructure d'information essentielle au Canada devrait presque toujours fournir un service fiable, accessible et sûr et que, si des pannes se produisent, elles n'auront qu'un impact limité sur le service global. Comme il a été amplement démontré ailleurs dans ce rapport, la réalisation de cet objectif ne sera pas un processus simple. Nous croyons qu'un ingrédient clé de cette réalisation sera l'attribution des responsabilités appropriées aux parties concernées. Nous reconnaissons également qu'il faut un travail additionnel sur des politiques publiques possibles avant que le gouvernement puisse agir en confiance quant aux résultats.

Au cours de notre recherche primaire et secondaire étendue sur les questions à régler, nous avons pu faire quelques observations préliminaires au sujet de modèles possibles de responsabilité. Nos observations ne sont pas exhaustives ni complètes dans leur couverture. Nous nous sommes plutôt fondés sur notre travail de recherche pour mettre en évidence les *dimensions* qui peuvent entrer dans le modèle de responsabilité de notre infrastructure d'information essentielle. En outre, nous signalons les *mécanismes* qui peuvent servir à établir, à appliquer et à exécuter les responsabilités voulues dans le domaine de notre infrastructure d'information essentielle.

13.1 Dimensions de la responsabilité

Il est pratiquement certain qu'un modèle universel de responsabilité ne serait pas efficace. Toutes les parties ne devraient pas être tenues d'assumer les mêmes responsabilités pour toutes les actions possibles. Un modèle de responsabilité efficace doit se concentrer sur des actions spécifiques, par les parties concernées, dans des conditions définies afin de déterminer les responsabilités qui devraient être assumées ou attribuées. Les *dimensions* présentées dans cette section proposent les voies à suivre pour identifier les responsabilités utiles.

13.1.1 Responsabilité pour le résultat… ou le processus?

Il y a une différence fondamentale et importante entre le fait de tenir un agent responsable d'un *résultat* plutôt que de le tenir responsable d'un *processus*. Dans la perspective de l'intérêt public, il est bien sûr intéressant de pouvoir identifier un agent et de le tenir responsable du résultat voulu. Il faut trouver l'agent et le rendre responsable du fonctionnement fiable, accessible et sûr de notre infrastructure d'information essentielle. Malheureusement, cela ne peut fonctionner que si l'agent a un degré raisonnable de contrôle sur les facteurs multiples qui contribuent à l'exploitation fiable, accessible et sûr de notre infrastructure d'information essentielle. Toutes les preuves laissent croire qu'on ne trouve pas de tels agents.

L'autre solution est de tenir les participants à la prestation des services de notre infrastructure d'information essentielle responsables des processus appropriés suivants. Plusieurs agents peuvent être tenus responsables des processus requis puisqu'ils contribuent à la prestation des services de l'infrastructure d'information essentielle. Si nous ne connaissons que les processus requis qui mènent au résultat voulu, alors l'attribution des responsabilités est relativement simple. Malheureusement, il n'y a aucune connexion blindée qui mène du processus au résultat voulu. Nous n'aurons peut-être pas d'autre option que de suivre les processus qui, dans la plupart des conditions, augmenteront la probabilité d'obtenir le résultat voulu.

13.1.2 Motifs d'acceptation de la responsabilité

Un particulier ou une organisation peut choisir d'être tenu volontairement responsable. Il y a presque toujours un intérêt personnel dans ces acceptations volontaires; l'ingénieur accepte certains types de responsabilités et il jouit en échange des droits et privilèges qui accompagnent le fait d'être reconnu comme un ingénieur. On trouve aussi couramment des particuliers ou des organisations qui acceptent des responsabilités car c'est un élément requis d'une relation souhaitable. Cela se voit souvent dans les relations entre les fournisseurs et leurs gros et puissants clients. Par exemple, Wal-Mart peut exiger certaines responsabilités de la part de ses fournisseurs et un bon nombre d'entre eux accepteront ces exigences car ils veulent faire affaire avec Wal-Mart ou ils en ont besoin. Finalement, tous les paliers de gouvernement ont plusieurs façons d'imposer les exigences de responsabilité aux particuliers et aux organisations qui se lancent dans certains types d'activités.

13.1.3 Parties qui acceptent la responsabilité

Le particulier peut être la partie qui est tenue responsable. C'est courant lorsque le particulier est un professionnel agréé au Canada. Les docteurs, les avocats, les comptables et les ingénieurs se voient comme des professionnels et ils acceptent certaines responsabilités en échange du droit d'exercer leur profession dans les provinces canadiennes. C'est également un exemple d'un groupe de particuliers – la profession – qui accepte et exécute les responsabilités parce qu'il veut être reconnu comme un groupe distinct avec des droits et des privilèges particuliers. Ce groupe représente le canal par lequel les responsabilités sont transmises aux membres individuels.

Les organisations de tous genres et de toutes tailles peuvent être tenues responsables. Il y a des exemples particulièrement intéressants d'organismes sans but lucratif qui sont tenus responsables des aspects du fonctionnement et de la gestion de l'infrastructure d'information mondiale et de la partie canadienne de cette infrastructure d'information. ICANN[299] a des responsabilités mondiales quant au fonctionnement et à la gestion des principales adresses Web, tout comme l'Agence canadienne d'enregistrement Internet (ACEI/CIRA)[300] au Canada. La Société Internet[301] est un autre exemple intéressant d'un organisme sans but lucratif qui joue un rôle clé dans la gestion et le développement de l'infrastructure d'information mondiale. Le propre réseau du Canada CANARIE[302] pourrait être un organisme canadien sans but lucratif de même nature.

13.1.4 Procédures de mise à exécution

Le but est d'éviter les défaillances dans le fonctionnement de notre infrastructure d'information essentielle. L'attribution des responsabilités à divers participants de notre infrastructure d'information essentielle constitue un moyen que le Canada peut utiliser pour s'assurer que notre infrastructure d'information essentielle continue de fournir les services requis. Que se passe-t-il lorsqu'un des participants ne s'acquitte pas de ses responsabilités? Qui remarque cela? Qui le signale? La mégapanne d'électricité de 2003 est un exemple intéressant des répercussions d'une panne. Dans ce cas, la panne était évidente – des millions de personnes ont été privées

[299]ICANN, *supra* note 281.
[300]CIRA, *supra* note 282.
[301]Voir en ligne : Internet Society <http://www.isoc.org/>.
[302]Voir en ligne : CANARIE <http://www.canarie.ca/>.

d'électricité à domicile et au travail. Déterminer *la* cause de la panne n'a pas été un processus facile[303].

Le réseau d'électricité de l'Amérique du Nord est un réseau relativement simple par rapport à l'infrastructure d'information de l'Amérique du Nord. La cause ou les causes des pannes dans le réseau d'électricité devraient être relativement faciles à déterminer. Avec notre infrastructure d'information essentielle, on ne peut jamais savoir ce qui a causé une panne importante, si ou au moment où une telle panne a lieu. Est-ce que nous revenons alors à la règle selon laquelle il n'y aucune exception pour les responsabilités assumées? Cela pourrait être dommageable car les participants ne tiendraient pas compte des responsabilités attribuées en les traitant de règles irréalistes imposées par un gouvernement qui ne comprend pas véritablement la situation.

13.1.5 Conséquences des défaillances

En tant que société, nous avons un certain nombre de façons dont nous pourrions imposer des pénalités à ceux qui ne s'acquittent pas de leurs responsabilités. Nous pourrions tourner en ridicule les particuliers ou les organisations. Une telle action publique pourrait avoir des conséquences graves sur la capacité du particulier ou de l'organisation à continuer de fonctionner. Elle pourrait pénaliser, mais n'offrirait aucune compensation. Comme autre solution, nous pourrions imposer des amendes ou des responsabilités en fonction des pertes subies à la suite du manquement aux obligations établies. Étant donné la portée et l'étendue de notre infrastructure d'information, même une « petite » défaillance pourrait entraîner une obligation financière énorme. Dans la perspective normale des choses, cela pourrait être un cas où la justice « naturelle » ne semble pas être rendue.

Le Canada pourrait également adopter l'approche de Sarbanes-Oxley[304] et de la loi 198 de l'Ontario[305], c'est-à-dire tenir les cadres supérieurs personnellement responsables du manquement aux procédures requises. Une peine maximale de cinq ans de prison serait vue par beaucoup comme un puissant moyen de dissuasion. Il y aurait des coûts associés au fait d'imposer une telle discipline à ceux qui fournissent l'infrastructure d'information essentielle au Canada. Ces coûts pourraient avoir un impact important sur la compétitivité mondiale du Canada. Et il n'est même pas certain que nous ayons les connaissances nécessaires à l'établissement des procédures requises pour ceux qui fournissent notre infrastructure d'information essentielle.

---

[303]Ce n'est pas à nous, ici, de fournir une analyse, même superficielle, de ce qui a causé la panne d'électricité de 2003.

[304]Voir en ligne : U.S. Securities and Exchange Commission - Spotlight on Sarbanes-Oxley Rulemaking and Reports <http://www.sec.gov/spotlight/sarbanes-oxley.htm>

[305]Voir « April 7, 2003 - Ontario responds to the *Sarbanes-Oxley Act* », en ligne : Gowlings News <http://www.gowlings.com/news/index.asp?intNewsId=107&strShowWhat=all>.

13.2 Mécanismes de responsabilité

Il y a un certain nombre de mécanismes avec lesquels on peut imposer des responsabilités. Ces mécanismes varient énormément quant à leur efficacité et à leur acceptation par la société. Le Canada pourrait lancer une campagne de publicité pour promouvoir l'acceptation volontaire de certaines responsabilités en relation avec notre infrastructure d'information essentielle. Des forces sociales pourraient être exercées. Par ailleurs, le Canada pourrait imposer de nouvelles exigences législatives à ceux qui fournissent des aspects de notre infrastructure d'information nationale. La loi pourrait servir à rendre exécutoires les responsabilités.

Nous soulignons de nouveau que cette section n'est pas un exposé complet des mécanismes possibles de responsabilité. Nous mettons en évidence certains des mécanismes observés au cours de notre recherche primaire et secondaire. Cet exposé est offert comme une proposition sur la gamme possible de mécanismes que le Canada pourrait envisager.

13.2.1 Défense de l'intérêt public

L'opinion publique a sûrement un impact sur les membres de notre société. L'opinion publique peut changer les prix des actions. L'opinion publique peut changer le flux des affaires pour les particuliers ou les firmes. L'opinion publique peut avoir des conséquences très graves pour tous les types d'organisations. Les gouvernements peuvent avoir un impact sur l'opinion publique de différentes façons. L'opinion publique doit être l'une des forces qui servent à accroître la volonté des participants d'accepter la responsabilité de leur rôle dans la prestation des services de notre infrastructure d'information essentielle. Mais l'opinion publique ne fera pas bouger tout le monde et son impact ne donnera pas toujours le comportement voulu car certains sont toujours « contre » par nature.

En dépit de toutes les limitations de la défense de l'intérêt public, notre recherche laisse croire que la volonté de nombreux participants d'accepter la responsabilité dépend essentiellement de l'opinion publique. Il est certain que si le public voit l'imposition des responsabilités comme des exigences sévères et déraisonnables du gouvernement, la résistance est probable et elle réussira probablement. L'opinion publique doit toujours être prise en considération dans n'importe quel plan d'attribution des responsabilités.

13.2.2 Achats prescrits

Tous les paliers de gouvernement exercent une influence considérable grâce à leurs décisions d'achat. Il y a un flux constant d'argent qui va des gouvernements à ceux qui fournissent notre infrastructure d'information. En fait, les affaires pour le compte du gouvernement représentent un élément vital des activités globales de nombreux fournisseurs de l'infrastructure d'information. Les gouvernements ont le pouvoir naturel d'agir comme tout client important et puissant; ils peuvent imposer leurs conditions à ceux qui veulent leur vendre des produits ou services.

Il y a des limitations évidentes quant aux pénalités que les gouvernements peuvent imposer aux manquements en matière de responsabilité. Les fournisseurs ont une réticence naturelle à accepter des contrats avec la possibilité de fortes pénalités. Et, jusqu'à présent, la plupart des fournisseurs de l'infrastructure d'information de l'Amérique du Nord ont réussi à éviter ce genre de contrats.

13.2.3 Établissement des normes

Il semble probable que quelques-unes des responsabilités souhaitables seront celles des normes de pratique suivantes. Dans le cas de notre infrastructure d'information essentielle, nous ne connaissons pas encore toutes les normes de pratique qui donneront les résultats voulus. Des normes de pratique prometteuses doivent être établies et testées sur le terrain. Le processus d'établissement des normes prend beaucoup de temps et beaucoup d'argent. Le gouvernement pourrait encourager de diverses façons l'établissement de normes de pratique qui sont particulièrement pertinentes pour l'infrastructure d'information essentielle.

Le gouvernement pourrait encourager et appuyer la participation des employés appropriés du gouvernement au processus d'établissement des normes. Le gouvernement pourrait encourager les ministères à être un milieu d'essais réels des normes de pratique proposées. Le gouvernement pourrait en financer d'autres pour le travail de développement ou financer d'autres organisations pour leur permettre de faire les essais en milieu réel. Et, dernier point mais non le moindre, le gouvernement pourrait demander l'acceptation des normes de pratique à ses propres ministères et à ses propres fournisseurs.

13.2.4 Application des normes

Le gouvernement a voix au chapitre quant à la façon dont un certain nombre de secteurs de notre société doivent fonctionner. Dans de nombreux cas, il a le pouvoir d'imposer des exigences sur la façon dont diverses activités sont exécutées au Canada. Dans la mesure où ce pouvoir est entre les mains du gouvernement, celui-ci pourrait l'utiliser pour mettre en vigueur l'application des normes de pratique appropriées. Il convient de noter, toutefois, que les normes de pratique ne peuvent pas être imposées arbitrairement s'il n'y a pas beaucoup de possibilités qu'elles soient adoptées avec succès. La communauté qui est censée suivre ces normes de pratique doit être « prête » à suivre les normes[306]. Il va falloir faire beaucoup de travail de « vente » des normes de pratique avant de les imposer à la communauté.

13.2.5 Autorisation d'exercer la profession

Il y a des possibilités et des défis propres au Canada en ce qui concerne l'autorisation d'exercer une profession (avec permis ou licence). Les professions au Canada sont de compétence provinciale. Les ordres professionnels reconnus sont des organisations provinciales. Chaque province, par exemple, a son propre ordre de génie. Il y a un certain degré de collaboration au niveau national, mais l'autorisation d'exercer est une affaire strictement provinciale. On reconnaît de plus en plus que les normes de pratique doivent être appliquées à l'échelle internationale, quelle que soit la portée provinciale de l'autorisation d'exercer. Les ingénieurs ont « résolu » le problème de l'accréditation nationale des programmes de diplômés en génie en acceptant volontairement de concentrer leurs efforts en un seul travail national d'accréditation[307].

---

[306]La dynamique qui mène à des normes « réussies » a été beaucoup étudiée par la communauté des normes internationales. L'approche adoptée par l'Organisation internationale de normalisation (<http://www.iso.org>) a été généralement une réussite. L'ISO essaie de recueillir les meilleures pratiques qui sont généralement suivies et de les reformuler comme guide de normalisation.

[307]Le Conseil canadien des ingénieurs (CCI/CCPE) (<http://www.ccpe.ca/>) a la responsabilité déléguée d'accréditer les programmes qui mènent à un diplôme de génie au Canada.

Avec l'autorisation d'exercer, nous faisons face à un défi national bien propre au Canada qui ne peut être réglé qu'à l'échelle provinciale. Nous faisons aussi face à une option typiquement canadienne, que l'on ne retrouve pas ailleurs, et qui est celle de reconnaître des droits de pratique réservés (ou restreints) largement applicables. Il existe un mécanisme, bien que ce soit au niveau provincial, d'appliquer le droit de pratique réservé, certainement en relation avec la pratique du génie. Le fait d'étendre cela aux aspects de notre infrastructure d'information essentielle pourrait être fort intéressant et attirer de nombreux ordres provinciaux de génie[308].

13.2.6 Réglementation des marchés

Le Canada a pris un certain nombre de mesures pour réglementer les marchés dans les limites de nos frontières. Les provinces ont fait de même chez elles. C'est au-delà de la portée de ce rapport que d'identifier les façons les plus prometteuses dont le marché des produits et services relié à notre infrastructure d'information essentielle peut ou devrait être réglementé. Notre but ici est d'indiquer que les marchés ne seront jamais complètement « libres ». L'État a toujours un rôle à jouer dans le fonctionnement des marchés à l'intérieur de ses frontières.

Il faudrait envisager d'utiliser les pouvoirs fédéraux et provinciaux pour réglementer les marchés en vue d'influer sur les modalités et conditions selon lesquelles les transactions relatives à notre infrastructure d'information essentielle sont permises. L'intérêt qu'il y a à utiliser l'approche indirecte pour la réglementation du marché est que les participants auront un certain choix quant au degré et à l'étendue auxquels ils sont prêts à participer à ce marché réglementé.

13.2.7 Réglementation directe

Dans les questions de bien public et de sécurité du public, l'État a le pouvoir considérable de réglementer ce qui est permis, ce qui est requis ou ce qui est interdit. De tels pouvoirs en matière de sécurité du public n'ont pas été traditionnellement utilisés pour réglementer directement notre infrastructure d'information, mais on pourrait soutenir fortement qu'une telle réglementation est nécessaire et appropriée. Nous reconnaissons que la possibilité d'une réglementation directe pourrait donner lieu à un vigoureux débat national[309] au sujet des mesures appropriées que le gouvernement doit prendre pour protéger notre infrastructure d'information essentielle. Mais il est vrai que notre infrastructure d'information est extrêmement importante pour la sécurité du public. Nous devrions peut-être envisager de pousser les Canadiens à se lancer dans un tel débat si, après une étude plus approfondie, il a été déterminé que la réglementation directe est une voie que le Canada devrait considérer.

13.3 Modèles de responsabilité

Le processus d'établissement de modèles de responsabilité pour notre infrastructure d'information essentielle est nécessairement complexe et il comporte plusieurs facettes. Tout ce que nous avons pu faire dans cette section du rapport, c'est de suggérer la portée et la gamme des dimensions et des modèles en matière de responsabilité.

---

[308]Communication privée d'un ancien président de l'Ordre des ingénieurs de l'Ontario (Professional Engineers of Ontario).

[309]Le débat aux États-Unis au sujet de la sécurité du territoire est représentatif de ce à quoi l'on pourrait s'attendre au Canada. Voir en ligne : Antiwar.com <http://www.antiwar.com/paul/paul39.html>.

14.0 Approches possibles pour l'amélioration de l'infrastructure d'information essentielle

Notre recherche a mis en évidence quatre volets qui méritent d'être considérés lorsqu'on cherche à améliorer la fiabilité, la sécurité et la fonctionnalité de l'infrastructure d'information essentielle. Ces propositions représentent la synthèse des opinions des principaux participants. Elles devraient toutes faire l'objet d'une recherche approfondie et de consultations étendues avant la mise en œuvre.

14.1 Encourager la diversité dans l'infrastructure d'information partagée

La diversité, encouragée de la manière appropriée, peut améliorer la fiabilité de l'infrastructure d'information globale du Canada. Il peut y avoir des avantages importants provenant de plusieurs instances de composants différents, distincts, mais équivalents sur le plan fonctionnel à chaque niveau de l'infrastructure d'information partagée.

Plusieurs arguments peuvent être avancés en faveur de la diversité. De nombreux participants clés que nous avons interrogés ont signalé les problèmes qu'ils voient dans le quasi-monopole de Microsoft sur les marchés de la bureautique et des systèmes d'exploitation de bureau. Notre recherche secondaire a appuyé fortement le point de vue bénéfique de la diversité. Notre conclusion est qu'il peut y avoir de grands avantages en matière de fiabilité qui découleraient d'une infrastructure d'information globale dans laquelle il y a une saine diversité sur le plan des composants et des fournisseurs.

Comme première étape, nous devrions mieux comprendre la véritable diversité des composants et des fournisseurs dans notre infrastructure d'information et, plus précisément, dans notre infrastructure d'information essentielle. Dans de nombreux sous-marchés, il y a déjà une diversité de fournisseurs et de composants installés. Aucun encouragement de la diversité ne serait requis ni justifié. Nous savons déjà quel est le manque de diversité dans le bureau. À quel autre endroit de notre infrastructure d'information essentielle y a-t-il un manque de diversité? Quels avantages pourraient en découler si on encourageait la diversité dans les secteurs où elle est absente actuellement?

Une fois que l'on a déterminé où la diversité serait bénéfique, des modèles pourraient être développés sur la meilleure façon d'atteindre les niveaux voulus de diversité. Dans les cas extrêmes, le gouvernement risque de ne pas avoir d'autre option pratique que de devenir lui-même un fournisseur de notre infrastructure d'information essentielle. Dans la plupart des cas, nous pensons que la diversité voulue pourrait être mieux réalisée avec une intervention moins énergique du gouvernement. Une surveillance continue pourrait être assurée par le gouvernement.

14.2 Appliquer la responsabilité dans l'infrastructure d'information partagée

Une plus grande responsabilité pourrait être attribuée à ceux qui bâtissent et exploitent les services partagés de l'infrastructure d'information. Comme ces services sont le résultat de mesures de collaboration de nombreux acteurs, la responsabilité sera probablement en grande partie celle des processus.

La première étape serait d'établir une image complète de tous ceux qui bâtissent ou exploitent un aspect des services partagés de l'infrastructure d'information du Canada. Étant donné le degré élevé d'interdépendance qui peut exister entre deux aspects de notre infrastructure d'information partagée, l'image devrait être complète; même un « petit » participant peut jouer un rôle absolument critique. On pourrait essayer en même temps de mieux cerner la nature critique de chaque participant dans la prestation de services fiables, accessibles et sûrs de l'infrastructure d'information essentielle.

Ce travail permettrait de mieux comprendre qui pourrait être tenu responsable. Une autre question à laquelle il faut répondre est celle de la nature de la responsabilité de chacun des participants. Peut-on identifier un résultat pour lequel le participant peut être tenu responsable? Dans la plupart des cas, les mesures de collaboration requises empêchent d'établir la responsabilité pratique en matière de résultats. L'autre solution est de tenir le participant responsable des processus appropriés suivants. Le défi consiste à identifier ou à développer les processus qu'il faut suivre pour atteindre le niveau voulu de sécurité, d'accessibilité et de fiabilité de notre infrastructure d'information essentielle. Ce ne sera pas une entreprise facile.

Après avoir déterminé qui peut être tenu responsable et pourquoi, il faut alors relever le défi d'appliquer les mesures appropriées et de s'assurer qu'elles se poursuivent. Dans la section 13, nous avons décrit quelques-uns des moyens à employer pour relever ce défi. La consultation avec ceux qui seront touchés doit être prudente. Cela représente un changement important dans la façon dont notre infrastructure d'information est développée, exploitée et gérée. Tout changement de cette ampleur sera probablement traumatique. Nous devrions nous préparer pour ce traumatisme probable.

14.3 Appliquer la responsabilité dans l'infrastructure d'information privée

Ceux qui exploitent des services privés qui assurent la connexion avec l'infrastructure d'information partagée pourraient être tenus plus responsables. Étant donné que ces services incombent en grande partie à ceux qui les exploitent, la responsabilité serait surtout appliquée pour les résultats. Les résultats sont en général mesurés de la meilleure façon possible à l'interface entre le service privé et l'infrastructure d'information partagée.

Les défis en matière de responsabilité pour les services privés correspondent à ceux des services de l'infrastructure d'information partagée. La première étape serait de comprendre quels services privés de quelles entités sont reliés à l'infrastructure d'information partagée. La gamme des services privés connectés est étendue et elle croît rapidement. Des millions d'ordinateurs au Canada se connectent déjà à notre infrastructure d'information partagée. Il y a des produits sur le marché aujourd'hui pour relier les automobiles, les appareils de chauffage, les caméras et les

téléphones à l'infrastructure d'information partagée. Et le réfrigérateur en ligne va bientôt être une réalité.

C'est déjà le cas que des virus informatiques se propagent à partir d'ordinateurs à domicile infectés. Le bruit d'un modem câble défectueux peut provoquer une grave détérioration du service pour tous les ordinateurs connectés au même segment de câble. Par ailleurs, il y a des réseaux privés canadiens avec des milliers d'appareils connectés. Les problèmes dans ces réseaux privés étendus peuvent avoir un impact qui se répercute sur toute l'infrastructure d'information canadienne. Nous devrions déterminer qui peut être responsable de cette « exportation » des problèmes dans l'infrastructure d'information canadienne plus étendue et nous devrions apprendre à bien évaluer la gravité de ces problèmes.

Avec cette information en main, nous serons en mesure d'établir les genres de responsabilités qui devraient être assumés et nous pourrons commencer à déterminer qui peut être tenu responsable. Ce qui est essentiel dans ce processus, c'est d'identifier la nature précise de la responsabilité qui pourrait être assumée. Quel est le comportement qui est requis ou interdit, le cas échéant, de la part du fournisseur ou du propriétaire d'un réfrigérateur en ligne? Comment pouvons-nous déterminer qu'il y a eu un bon comportement? Quelles sanctions pourraient être raisonnablement imposées au fournisseur ou au propriétaire d'un réfrigérateur défectueux? L'exemple du réfrigérateur est quelque peu léger, mais les mêmes questions pourraient être posées à la compagnie qui a des milliers d'appareils connectés à un réseau qui traverse le Canada.

« Tout » ce qu'il reste à faire, c'est de réaliser cela d'une façon rapide qui est considérée juste par toutes les parties concernées. Ce n'est pas un mince exploit. Le succès complet est peu probable, mais nous pouvons faire des progrès en réduisant les risques d'atteinte à notre infrastructure d'information partagée de la part des services privés connectés. Les enjeux sont élevés. Des mesures significatives et informées seraient bénéfiques.

14.4 Encourager l'établissement et l'adoption de normes

En général, les normes sont utiles pour la mise en œuvre de la responsabilité. Les normes nous permettent de mesurer, de certifier et d'interconnecter des éléments de l'infrastructure d'information. Les normes internationales peuvent être les plus importantes à cause de la nature mondiale de l'infrastructure d'information, mais les normes canadiennes peuvent également jouer un rôle important.

Les normes d'interconnexion de base fonctionnent remarquablement bien. Toute personne ou chose qui veut se connecter peut le faire et les normes minimales requises d'interconnexion sont bien connues. Il y a d'autres normes de réseau qui sont moins bien connues et qui sont mises en œuvre de façon moins uniforme. Quelques-unes de ces normes pourraient être des facteurs importants lorsqu'il s'agit de préserver notre infrastructure d'information essentielle en cas de perte sélective d'une capacité globale du réseau. Par exemple, le nouveau protocole Internet (IPv6) comprend un moyen pour les paquets de demander un service prioritaire. Avec IPv6 en place, il serait possible en cas de panne partielle de l'infrastructure d'information de réserver toutes les capacités restantes afin de répondre aux besoins de notre infrastructure d'information essentielle. Il y a un certain nombre d'autres normes qui pourraient également servir à préserver le service de notre infrastructure d'information essentielle.

Des travaux pourraient être entrepris pour déterminer les normes les plus prometteuses à adopter pour préserver le service de notre infrastructure d'information essentielle. De façons différentes, les trois suggestions précédentes dépendent toutes de l'identification ou de l'établissement de normes de produits ou de processus et du fait de s'assurer qu'elles sont appliquées en pratique. Le défi à relever pour les normes comporte plusieurs facettes :

- Identifier les normes les plus importantes pour une infrastructure d'information essentielle fiable, accessible et sûre.
- Travailler au sein de la communauté des normes internationales à l'établissement et à la mise à jour de ces normes clés.
- Soutenir l'adaptation et l'adoption de ces normes clés pour qu'elles soient utilisées en relation avec notre infrastructure d'information essentielle.
- Encourager ou exiger l'utilisation de ces normes clés par ceux qui bâtissent ou exploitent notre infrastructure d'information globale.

Dans ce contexte, il y a une option typiquement canadienne pour les normes. Nos diverses lois provinciales sur le génie donnent aux ingénieurs canadiens le droit exclusif à des domaines de pratique réservés (ou restreints). Ce mécanisme, offert uniquement au Canada, pourrait servir à assurer l'application des normes clés.

15.0 Lacunes du savoir

Un certain nombre de fois dans le présent rapport, nous avons souligné le fait que la société dépend de plus en plus de l'existence et de l'exploitation appropriée de l'infrastructure d'information essentielle. Toutes les autres infrastructures essentielles, soit celles du réseau d'électricité, de transport, des services financiers, etc., dépendent fortement de cette infrastructure d'information. Ainsi, la continuation et l'évolution positive progressive de l'infrastructure d'information essentielle comme entité viable et solide ont une importance primordiale, à la fois pour le Canada et pour le reste du monde.

Le fonctionnement et la croissance de l'infrastructure d'information essentielle dépendent en grande partie des fournisseurs de logiciels et de systèmes TI. Toutefois, dans la plupart des cas, ces entités ont un très faible niveau de responsabilité légale par rapport aux produits et aux services qu'elles offrent. Cette disparité devient encore plus évidente si nous comparons leur niveau de responsabilité à celui des fournisseurs de produits et services dans d'autres secteurs d'infrastructure essentiels.

Si l'infrastructure d'information essentielle doit continuer à évoluer et à se développer sur le plan des fonctionnalités, de la solidité et de la sécurité, nous devrions envisager les mérites qu'il y a à améliorer la gouvernance globale et la responsabilité dans le domaine de l'infrastructure d'information essentielle. Nous serons en bien meilleure position pour envisager une telle amélioration si nous comblons les lacunes critiques de notre savoir. Quelques-unes de ces lacunes sont indiquées ci-dessous comme projets éventuels de recherche.

La liste ci-dessous vise à être représentative et non exhaustive. Nous reconnaissons également qu'il y a des aspects communs dans ces suggestions de projets et que les calendriers de ces projets peuvent chevaucher des années financières. Avant d'entreprendre un projet donné, nous recommandons de faire un examen préalable afin de s'assurer qu'il n'y a pas d'autres initiatives en cours qui font double emploi.

15.1 Répertoire des participants

Énoncé de travail
Il faut établir un répertoire des principaux participants dans l'infrastructure d'information essentielle, y compris la sphère d'influence et de préoccupations de chacun d'eux. Cela ferait partie de l'information essentielle au lancement du processus qui vise à établir un vaste consensus dans le cas de changements proactifs à la responsabilité dans le domaine de l'infrastructure d'information essentielle.

Justification
Il serait important d'avoir une bonne connaissance de travail des intérêts, des objectifs, des priorités et des perceptions des principaux participants au moment de définir les changements qui pourraient améliorer et étendre à l'avenir la responsabilité dans le domaine de l'infrastructure d'information essentielle. L'une des étapes pour obtenir le consensus des participants serait d'identifier et de catégoriser clairement ces participants en fonction de leurs objectifs, programmes et priorités.

15.2 Étude initiale de cas

Énoncé de travail
Il faut mener une étude de cas qui définit une fonction fournie par l'infrastructure d'information essentielle et qui est nécessaire au soutien d'un autre secteur critique. Toute l'infrastructure d'information qui assure cette fonctionnalité doit être identifiée. Une analyse doit être fournie qui met en évidence les parties de cette tranche d'infrastructure la plus vulnérable aux pannes.

Justification
L'identification des maillons les plus faibles des diverses parties de l'infrastructure d'information essentielle est importante à cause de l'interdépendance des différents segments de l'infrastructure d'information essentielle. En outre, cette infrastructure sert de fondation à de nombreux autres secteurs de toute l'infrastructure essentielle nationale.

15.3 Autres études de cas

Énoncé de travail
Il faut mener une série d'études de cas, comme l'étude indiquée dans la section précédente, sur l'infrastructure d'information essentielle qui supporte une série d'autres segments d'infrastructure essentiels. Il faut analyser les maillons faibles pour déterminer les points communs entre les segments.

Justification
La raison d'être de cette section, c'est essentiellement de reformuler ce qui a été traité dans la section précédente. De plus, une fois que les points communs de tous les segments de l'infrastructure d'information essentielle sont déterminés et analysés, il devrait être plus facile d'identifier les points de défaillance les plus probables et les scénarios de panne. En outre, cette connaissance pourrait aider à établir les solutions possibles qui élimineraient ou renforceraient les maillons faibles de l'infrastructure d'information essentielle.

15.4 Défaillances de l'infrastructure d'information

Énoncé de travail
Il faut faire des recherches pour compléter/développer le diagramme suivant :

Table 15.1 Défaillances de l'infrastructure d'information essentielle et impacts sur la santé et la sécurité

Catégorie	Incident(s)	Morts/blessures alléguées	Licence(s) en vigueur	Lois ou règlements pertinents
Transport aérien	Écrasement de l'hélicoptère Chinook			
Défense	Panne du missile Patriot			
Santé	Médecine nucléaire – Machine d'irradiation Therac-25			
Autres	Données			

Justification
Comme il a été discuté dans ce rapport, l'un des principaux éléments de motivation pour que le secteur public intervienne en matière de responsabilité dans l'infrastructure d'information essentielle pourrait être la présence de questions majeures de santé et de sécurité. Cette initiative de recherche permettra d'identifier ces domaines. Elle pourrait aussi fournir de l'information sur toutes les lois ou tous les règlements pertinents.

15.5 Établissement de la métrologie des performances

Énoncé de travail
Il faut examiner l'état actuel de l'analyse/de la mesure des performances de l'infrastructure d'information essentielle et de ses réseaux, systèmes et composants associés. Des hypothèses doivent être faites sur l'évolution possible des normes de performance. Cela comprend à la fois les normes de processus et les normes de résultats. Il convient de proposer des méthodologies et des cadres de travail possibles qui sont nécessaires à l'établissement de ces normes. En sachant que la définition des normes est une tâche très complexe et très ardue, comment allons-nous procéder?

Justification
Avant d'essayer d'évaluer les mesures de sécurité de l'infrastructure d'information essentielle, nous devrions avoir une idée des niveaux prévus de performance des composants et des systèmes qui constituent l'infrastructure d'information essentielle. Avant même de traiter de la responsabilité, nous devrions nous poser la question : responsables de quoi? Actuellement, nous gênés par notre incapacité à mesurer les éléments de façon uniforme. Il faudrait tenir compte à la

fois des normes de processus et des normes de résultats. Étant donné que l'Internet est un réseau mondial, des normes mondiales uniformes devraient être établies et mises en œuvre.

15.6 Établissement de la métrologie de la sécurité

Énoncé de travail
Il faut examiner l'état actuel de l'analyse/de la mesure de la sécurité de l'infrastructure d'information essentielle et de ses réseaux, systèmes et composants associés. Les défectuosités et les lacunes devraient être identifiées. Des théories seront établies quant à l'évolution future de l'évaluation et de l'analyse de la sécurité. Il convient de proposer des méthodologies et des cadres de travail nécessaires à l'établissement de ces outils et méthodes de mesure de la sécurité.

Justification
Pour l'instant, nous ne pouvons pas véritablement quantifier le niveau de sécurité inhérent dans l'infrastructure d'information essentielle, ni ce que le niveau optimal devrait être. Nous devrions envisager de définir à la fois les normes des tests de sécurité et les normes des processus de sécurité. Ces normes doivent être définies et mises en œuvre à l'échelle mondiale. Nous pouvons essentiellement vouloir l'équivalent fonctionnel des Principes comptables généralement reconnus (PCGR/GAAP) pour la mesure et l'évaluation de la sécurité de l'infrastructure d'information essentielle.

15.7 Connaissances du public en matière de droit cybernétique

Énoncé de travail
Il faut faire un sondage auprès du grand public afin de déterminer le niveau actuel de sensibilisation et de préoccupation en matière de droit cybernétique.

Justification
Des preuves anecdotiques nous laissent croire que le niveau de sensibilisation et de préoccupation du grand public en matière de droit cybernétique est assez faible. C'est particulièrement important à la lumière du niveau élevé de dépendance de la société envers l'infrastructure d'information essentielle. Nos législateurs risquent de ne pas être très motivés pour améliorer et réformer les lois applicables si le niveau de sensibilisation du public, et donc la conformité, est faible.

15.8 Communication du droit cybernétique au public

Énoncé de travail
Si le sondage mentionné ci-dessus permet de s'assurer que le niveau actuel de sensibilisation du public en matière de droit cybernétique est faible, des recherches ultérieures pourraient aider à déterminer les meilleures méthodes pour rehausser ce niveau grâce à la communication. Les méthodes choisies devraient être à la fois faisables et efficaces.

Justification
On s'est rendu compte récemment que même les professionnels qui travaillent dans les domaines directement touchés par le droit cybernétique ne saisissent pas véritablement l'état actuel de la loi[310]. Cela comprend les cadres supérieurs de l'Association de l'industrie canadienne de l'enregistrement, les musiciens professionnels, les journalistes qui se spécialisent dans ce domaine et ainsi de suite. Il n'est donc pas logique ni même raisonnable de s'attendre à ce que le grand public puisse comprendre ce régime légal hautement complexe.

15.9 Communication du droit cybernétique aux corporations

Énoncé de travail
Les corporations se composent de personnes et quelques-unes des idées de la section précédente peuvent donc s'appliquer ici aussi. Toutefois, les corporations peuvent nécessiter des mécanismes additionnels de responsabilité tels que :

1. L'auto-certification
2. Des tests/des certifications de tiers

Il faut mener une étude pour évaluer l'efficacité des méthodologies proposées ci-dessus. Il convient de déterminer dans quelles circonstances les diverses options devraient être utilisées (c'est-à-dire, quand, où, comment?).

Justification
Comme il a été mentionné précédemment, les corporations sont composées de personnes et la section 15.1.9 s'applique donc également aux corporations. Toutefois, si la législation et/ou la réglementation (par exemple, la loi *Sarbanes-Oxley Act of 2002* aux États-Unis) sont employées afin de prévenir certains comportements, des mécanismes additionnels de responsabilité peuvent être requis. En ce qui concerne les corporations, la conformité doit être rendue explicite, plutôt qu'implicite.

15.10 Tendances dans les activités criminelles cybernétiques

Énoncé de travail
Il faut mener des recherches afin de classifier les types d'infractions relevés. Les niveaux et les types de crimes cybernétiques du passé et d'aujourd'hui doivent être déterminés. Des projections et des estimations du type et de la quantité des crimes cybernétiques doivent être faites.

Justification
Il est important d'évaluer l'impact de chaque type d'infraction cybernétique sur l'infrastructure d'information essentielle.

[310]Shane Schick, « How the downloading debate is starting to infect other areas of IT »,*IT Business*, (2 mars 2004), en ligne : itbusiness.ca <http://www.itbusiness.ca/index.asp?theaction=61&sid=54933#>.

15.11 Le droit criminel comme élément dissuasif du crime cybernétique

Énoncé de travail
Il faut mener une recherche primaire pour déterminer comment le droit criminel actuel peut être réformé/modifié afin de traiter et de prévenir efficacement le crime cybernétique. Cela comprendrait sans doute des entrevues avec des avocats et des psychologues spécialisés dans le domaine, des travailleurs auprès des jeunes, du personnel chargé de l'exécution de la loi, etc.

Justification
Le régime actuel du droit criminel a eu de la difficulté à suivre le même rythme que les projets technologiques rapides et les changements inhérents dans notre société dominée par l'ordinateur et l'information. En outre, la nature unique de l'information combinée à la nature internationale/sans frontières du crime cybernétique, a imposé des exigences au droit criminel traditionnel qui sont difficiles à traiter efficacement. Le *Code criminel* a été établi pour servir un monde de « biens tangibles » et il n'est pas aussi bon pour traiter des infractions liées à l'information dans le cyberespace.

De plus, les deux principaux types de cyber-criminels que nous avons identifiés ne semblent pas être véritablement dissuadés par le régime criminel courant. Les cyber-criminels novices ne comprennent pas ou ne réalisent pas qu'ils peuvent être arrêtés pour leurs crimes assistés par ordinateur. À l'autre extrémité du spectre, on trouve les cyber-criminels professionnels qui utilisent leur expertise technique pour minimiser les risques d'être attrapés. En outre, ils sont prêts à assumer ce risque dans le « cadre de leurs affaires ».

15.12 L'évolution de la cyber-assurance

Énoncé de travail
La section 9.4 donne un bref aperçu du potentiel de la cyber-assurance. Étant donné que seuls les faits saillants sont explorés, il peut être utile d'étudier ce sujet de manière beaucoup plus approfondie. Les divers types de cyber-assurance pourraient être explorés à la lumière de leurs forces et de leurs faiblesses et on pourrait étudier également leur applicabilité aux divers composants de l'infrastructure d'information essentielle.

Justification
Il est utile d'en arriver à un consensus sur l'évolution de la cyber-assurance dans le domaine de l'infrastructure d'information. Quelle que soit l'orientation suivie, elle devrait être compatible avec les forces prédominantes du marché de façon à encourager un développement rapide et efficace des produits et services d'assurance appropriés.

15.13 Droit de la responsabilité du fait des produits dans le domaine du logiciel

Énoncé de travail
Il faut mener une étude sur l'état actuel (et l'état futur possible) du droit de la responsabilité du fait des produits dans le domaine du logiciel.

On pourrait déterminer les lacunes critiques du savoir qui doivent être comblées afin d'accélérer l'évolution positive de la responsabilité dans le domaine de l'infrastructure d'information. Des

secteurs à surveiller sur une base permanente seront également suggérés et des techniques de surveillance proposées.

Justification
Étant donné que le logiciel est généralement sous licence, la propriété du programme revient au fabricant. Cela s'applique à la fois au logiciel commercial et au logiciel personnalisé. Comme aucun produit n'est véritablement acheté, il est possible que les notions de la common law sur l'adaptation des objets, les dispositions de la *Loi sur la vente d'objets* ou d'autres lois de protection du consommateur aient une utilité limitée lorsqu'elles s'appliquent à un fabricant de logiciels.

15.14 Autorisation d'exercer (permis ou licence) pour les spécialistes du logiciel

Énoncé de travail
Il faut mener des recherches pour étudier la question de savoir si les spécialistes du logiciel devraient avoir l'autorisation d'exercer ou non ou encore être certifiés ou réglementés d'une manière quelconque. Devraient-ils être réglementés, comme le sont les ingénieurs? L'autoréglementation est-elle une possibilité, comme dans le domaine des soins de santé?

Justification
En ce qui concerne les diverses spécialisations du génie, il a fallu des catastrophes majeures (par exemple, des écrasements de ponts) pour rendre la certification obligatoire. Il serait plus prudent d'aborder la question de la réglementation des spécialistes du logiciel de manière proactive au lieu d'attendre qu'il y ait une catastrophe due à une défaillance du logiciel et de réagir par la suite (par exemple, une panne de segments de l'infrastructure d'information essentielle qui aurait pour résultat des pertes de vie).

15.15 Attribution des responsabilités dans l'infrastructure d'information essentielle

Énoncé de travail
Il faut mener une étude pour clarifier et déterminer comment les niveaux actuels de responsabilité associés aux divers participants de l'infrastructure d'information essentielle touchent le fonctionnement et le développement de l'infrastructure d'information essentielle. Ces divers niveaux de responsabilité devraient être associés aux aspects à la fois souhaitables et indésirables de l'infrastructure d'information essentielle en place. Quelles leçons peut-on en tirer et comment cette information peut-elle être utilisée pour créer à l'avenir une infrastructure d'information essentielle plus solide et plus fonctionnelle?

Justification
Il semble y avoir une vaste gamme de niveaux de responsabilité (ou de manque de responsabilité) dans l'infrastructure d'information essentielle. En étudiant ce phénomène de façon rigoureuse, nous pourrons normaliser et améliorer le niveau global de responsabilité ainsi que la fiabilité et la solidité de la future infrastructure d'information essentielle.

15.16 Attributs de l'infrastructure d'information essentielle actuelle/future et leurs implications

Énoncé de travail

Il faut mener des recherches pour déterminer quels sont les attributs connus de l'infrastructure d'information essentielle actuelle. Quelles sont les relations entre ces attributs? Comment l'état voulu de la future infrastructure d'information essentielle est-il lié à chacun de ces attributs? Comment les divers attributs de l'infrastructure d'information essentielle sont-ils liés aux politiques qui régissent l'infrastructure d'information essentielle?

Justification

En étant en mesure d'évaluer avec précision les attributs de l'infrastructure d'information essentielle en place et d'avoir une bonne connaissance de travail de ces attributs, à la fois souhaitables et indésirables, on peut tirer des leçons quant à la façon d'améliorer l'infrastructure d'information essentielle future. En outre, en étudiant les relations entre les attributs et les politiques qui régissent l'infrastructure d'information essentielle, il sera possible d'établir de nouveaux paradigmes de responsabilité et d'améliorer les paradigmes actuels pour la future infrastructure d'information essentielle.

15.17 Questions de confidentialité et vulnérabilités de l'infrastructure d'information essentielle

Énoncé de travail

Il faut mener des recherches sur la façon dont l'information concernant les menaces et les vulnérabilités de l'infrastructure d'information essentielle peut être diffusée et partagée entre le secteur privé et les organismes d'exécution de la loi tout en protégeant la vie privée des particuliers (ou en minimisant les violations de cette vie privée).

Justification

On a déjà déclaré qu'il faut une réponse multidisciplinaire[311] pour régler les problèmes de l'infrastructure d'information essentielle. Outre les solutions proposées sur le plan technique, de la gestion, de l'éducation du public et ainsi de suite, la collecte et le partage de l'information entre les organismes d'exécution de la loi et le secteur privé peuvent être requises si des solutions doivent être établies pour régler les vulnérabilités actuelles de l'infrastructure d'information essentielle. Toutefois, une telle utilisation secondaire de l'information soulève invariablement de sérieuses préoccupations quant à la protection de la vie privée. En faisant les recherches, on pourrait examiner des façons de partager l'information qui auront un impact minimal sur la vie privée des particuliers.

[311]Patterson & Personick, *supra* note 181 à 61.

16.0 Remarques finales

L'infrastructure d'information essentielle ne ressemble à aucune autre infrastructure essentielle :

- C'est la seule infrastructure où la partie essentielle est définie comme celle qui supporte les autres infrastructures essentielles.
- Les frontières de l'infrastructure d'information essentielle sont indéterminées et évolutives et elles ont de nombreuses interdépendances indirectes.
- La complexité et le dynamisme de l'infrastructure d'information essentielle dépassent de loin ce que l'on trouve dans toutes les autres infrastructures essentielles.

On a avancé de nombreuses propositions simples pour atteindre le niveau voulu de fiabilité, d'accessibilité et de sécurité dans notre infrastructure d'information essentielle. L'examen le plus superficiel des questions présentées dans la section 11 de ce rapport valide la maxime selon laquelle : « Les problèmes complexes ont des réponses qui sont simples, faciles à comprendre … et fausses! »

Malgré tous les défis, le Canada a la responsabilité de trouver la meilleure réponse possible à la question : « Comment nous, en tant que nation et société, pouvons le mieux augmenter la fiabilité, l'accessibilité et la sécurité de l'infrastructure d'information essentielle de laquelle nous dépendons? »

À notre avis, voici les grandes lignes à suivre :

1. Développer une meilleure compréhension, plus détaillée, de l'infrastructure d'information essentielle;
2. Établir de meilleurs moyens de mesurer les performances de l'infrastructure d'information essentielle;
3. Choisir les meilleures solutions de compromis, et les plus éclairées, entre les coûts et les risques;
4. Concentrer nos efforts sur les aspects les plus faibles de l'infrastructure d'information essentielle et
5. Reconnaître que la vigilance est un processus continu dans notre infrastructure d'information essentielle.

C'est un programme ambitieux, mais c'est un défi que nous ne relevons pas au péril de notre nation et de notre société. « Continuer comme si de rien n'était » n'est pas une solution. Nous devons faire preuve de courage et de leadership. C'est dans le meilleur intérêt de tous les Canadiens d'avoir une infrastructure d'information essentielle fiable, accessible et sûre.

Bibliographie

680 News Staff. (2004). “Parts of Microsoft source code leaked over Internet, software giant says.” http://www.680news.com/news/business/article.jsp?content=b0212154A (13 February 2004).

ADP Canada. (2004). “ADP Solutions and Services”. http://www.adp.ca/en/index.html (5 March 2004).

Alderson, Douglas and Deanne Montesano. (2003). *Regulating, De-regulating and Changing Scopes of Practice in the Health Professions – A Jurisdictional Review* (a report prepared for the Health Professions Regulatory Advisor Council (HPRAC) at 3, http://www.oaccpp.on.ca/news/appendix1-dp.pdf (12 February 2004).

Anderson, Robert H. *et al*. *The Global Course of the Information Revolution: Technological Trends: Proceedings of an International Conference* Santa Monica: RAND, 2001.

Anderson, Ross. (2001). “Why Information Security is Hard – An Economic Perspective.” (Proceedings of the 17th Computer Security Applications Conference, New Orleans, Louisiana, Dec. 2001). *Annual Computer Security Applications Conference*. http://www.acsac.org/2001/papers/110.pdf (16 February 2004).

Anton, Philip S., Silberglift, Richard & James Schneider. *The Global Technology Revolution – Bio/Nano/Materials Trends and Their Synergies with Information Technology by 2015, A Report Prepared for the National Intelligence Council by RAND National Defence Research Institute*. Santa Monica: RAND, 2001.

Apicella, Mario. “Shaking hands is not enough.” *InfoWorld* Vol. 23, No. 18 (30 April 2001): pp. 49-53.

Arce, Iván. (2004). “More Bang For the Bug: An Account of 2003’s Attack Trends.” *IEEE Security & Privacy*. http://www.computer.org/security/v2n1/j1att.htm (12 March 2004).

Arkin, Ofir. (2002). Atstake Corporate White Paper. “Trace-Back: A Concept for Tracing and Profiling Malicious Computer Attackers.” pp. 1–17. http://www.atstake.com (30 December 2003).

Associated Press. (2004)“Chinese standards don't work with Intel.” *The Globe and Mail*. http://www.globetechnology.com/servlet/story/RTGAM.20040311.gtwifimar11/BNStory/Technology/ (11 March 2004).

Baase, Sara. (1974). “IBM: Producer or Predator.” *Reason* (April 1974) pp. 4–10. http://www-rohan.sdsu.edu/faculty/giftfire/ibm.html (03 March 2004).

Bace, Rebecca, Geer, Daniel, Gutmann, Peter, Metzger, Perry, Pfleeger, Charles P., Quarterman, John S., and Bruce Schneier. (2003). "Cyber*In*security: The Cost of Monopoly – How the Dominance of Microsoft's Products Poses a Risk to Security." http://www.ccianet.org/papers/cyberinsecurity.pdf (2 February 2004).

Banisar, David. "Perspective: manufacturers should be liable when computer bugs leave consumers in the lurch." *Regional Review* Vol. 12, No. 3 (September 2002): pp. 2–5.

Banisar, David. (2001). "Save the Net, Sue a Software Maker." http://www.securityfocus.com/columnists/47 (9 February 2004).

Baptista, Joe. (2002). "Electronic privacy issues affecting Canadians, business and government". (Letter to Privacy Commissioner of Canada re: Internet Root Servers). http://cecua.customer.netspace.net.au/Acrobat1/Root%20Server%20Privacy%20Complaint.pdf (3 February 2004).

Baran, Paul. (1964). "On Distributed Communications." *The Rand Corporation*. http://www.rand.org/publications/RM/RM3420/index.html (14 February 2004).

Barrett, Jennifer. (2004). "More Doom? The infection rate for the world's fastest growing email virus ever is subsiding, but security experts say the risk of new attacks is not." *Newsweek*. http://www.msnbc.msn.com/id/4154289 (4 February 2004).

Barrett, Jennifer. (2004). "We're Making Rapid Progress." *Newsweek*. http://msnbc.msn.com/id/4100822/ (4 February 2004).

Barrett, Katherine. 2002. Food Fights: Canadian regulators are under pressure to face the uncertainties of genetically modified food. *Alternatives Journal*. Vol. 28, No. 1: 28–33.

Bennett, Elizabeth. (2003). "Improving Your Bottom Line – Certifiably." *Baseline Magazine*. http://www.baselinemag.com/article2/0,3959,1408933,00.asp (13 January 2004).

Berlind, David. (2004). "Greed: the real reason for Sobig and MyDoom's "success." ZD Net Tech Update. http://techupdate.zdnet.com/techupdate/stories/main/the_real_reason_for_Sobig_and_MyDoom_success.html (9 February 2004).

Berlind, David. (2004). "Instead of indemnification, consider 'open source insurance'." *ZD Net Tech Update.* http://techupdate.zdnet.com/techupdate/stories/main/open_source_insurance_print.html (24 February 2004).

Berlind, David. (2004). "Phishing: Spam that can't be ignored." *ZD Net Tech Update.* http://techupdate.zdnet.com/techupdate/stories/main/Phishing_Spam_that_cant_be_ignored_print .html (13 January 2004).

Berlind, David. (2004). “The SCO legal train: Know your options.” *ZD Net Tech Update.* http://techupdate.zdnet.com/techupdate/stories/main/SCO_legal_train_print.html (24 February 2004).

Blakely, Stephen. “Left in the dark about power failures.” *Nation's Business* Vol.85, No. 6 (June 1997): p. 74.

Blanchfield, Mike and Rick Mofina. “Canada's cyber network, pipelines and power grids, which are all tied to the United States, are the most likely targets of terrorists exercising vendettas against America.” *Can West News*. (21 December 1999).

Bloor, Robin. (2004). “The Lawyers are coming.” *IT-Analysis.com*. http://www.it-analysis.com/article_pf.php?articleid=11666 (13 February 2004).

Blue Ribbon Advisory Panel on Cyberinfrastructure. (2003). *Revolutionizing Science and Engineering Through Cyberinfrastructure: Report of the National Science Foundation Blue Ribbon Advisory Panel on Cyberinfrastructure*. http://www.communitytechnology.org/nsf_ci_report/ (8 January 2004).

Bohnen, Linda S. *Regulated Health Professions Act- A Practical Guide*. Toronto: Canada Law Book, 1994.

Bowen, Jonathan P., Isaksen, Ulla, and Nimal Nissanke. (1996). “System and Software Safety in Critical Systems.” http://www.museophile.lsbu.ac.uk/pub/jpb/scs-survey-tr97.pdf (3 February 2004).

Boyd, Clark. (2003). “Cyber threats risk net's future.” *BBC News UK Edition*. http://news.bbc.co.uk/1/hi/technology/3322449.stm (19 December 2003).

Bradley, Patrick E. and Jennifer R. Smith. 2000. Liability for Software Defects. New Jersey Law Journal. Vol. 62, No. 1: 3–9.

Brewin, Bob. (2003). “Industry and gov't call for U.S.-wide cattle ID system.” *IT World Canada*. http://www.itworldcanada.com/Pages/Docbase/ViewArticle.aspx?ID=idgml-c5bdcf2d-148f-4f1f-a2a9-b18e20ec942f&Portal=E-Government (5 January 2004).

Bridis, Ted. (2004). “Microsoft Warns on Windows Security Flaws.” http://apnews.myway.com//article/20040210/D80KJ01G1.html (11 February 2004).

Bridis, Ted. (2004). “Microsoft Warns Windows Prone to Hacking.” http://apnews.myway.com/article/20040211/D80L3AD80.html (11 February 2004).

British Telecommunications, PLC (BT). (2003). BT's Response to OFTEL's Consultative Document: "Encouraging self- and co-regulation in telecoms to benefit consumers." http://www.btplc.com/pda/Corporateinformation/Regulatory/RegulatoryInformation/OftelConsultativeDocuments/SelfRegulationSept2000/response.pdf (19 February 2004).

Brown, Alan S. 2002. SCADA vs. the Hackers: can freebie software and a can of Pringles bring down the U.S. power grid? Mechanical Engineering-CIME. Vol. 124, No. 12: 37–41.

Bruce, P. James. (2003). "Disaster Mitigation and Preparedness in a Changing Climate." http://www.ocipep.gc.ca/research/scie_tech/disMit/disMit/disas_miti_e.asp (30 December 2003).

BTexact Technologies (a division of British Telecommunications). (2001)."Technology Timeline." http://www.btexact.com/docimages/42270/42270.pdf (5 March 2004).

Business Week Staff. "The Best Way to make Software Secure: Liability." *Business Week* Vol./No. 3774 (18 March 2002): p. 61.

Business Week Staff. "This Law is User-Unfriendly." *Business Week* Vol./No. 3677 (17 April 2000): pp. 94–97.

Buxton, J. M., Naur, Peter, and Brian Randell, eds. Software Engineering: Concepts and Techniques. New York: Petrocelli/Charter, 1976.

Callahan, Dennis. (2004). "Sarbanes-Oxley: Road to Compliance." *EWeek-Enterprise News and Reviews*. http://www.eweek.com/article2/0,4149,1527933,00.asp (17 February 2004).

Campus Information Technologies and Educational Services. (2004). *Glossary of Acronyms and Technical Terms*. http://www.cites.uiuc.edu/glossary/#i. (22 February 2004).

Canadian Broadcasting Corporation. (2004). "Computer Invasion: A History of Automation in Canada." *CBC Archives* http://archives.cbc.ca/IDD-1-75-710/science_technology/computers/ (26 February 2004).

Canadian Community Reinvestment Coalition. (1997). "An Accountability System For Financial Institutions in Canada: How To Ensure They Meet a High Standard of Performance." *CCRC Position Paper #5*. http://www.cancrc.org/english/posdoc5eng.html (December 1997).

Canadian Community Reinvestment Coalition. (2001). "Comparison of Amendments set out in Bill C-8 to Financial Institution and other Laws vs. CCRC Recommendations." http://www.cancrc.org/english/recomm01.html (19 February 2004).

Canadian Press. (2004). "Ottawa not ready for emergency, documents show." *The Globe and Mail*. http://www.theglobeandmail.com/servlet/story/RTGAM.20040111.wblack0111/BNPrint/National/ (13 January 2004).

CANARIE. *A Nation Goes Online – Canada's Internet History*. Montreal: CA*net Institute, 2001. http://www.canarie.ca/press/publications/ango.pdf (3 March 2004).

Carey, David (interviewer). “Inside Microsoft: helming IT at software's ground zero [Interview with John Connors].” *Information Technology Management* Vol. 7, No. 4(1999): pp. 22–32.

Carlson, Caron. (2003). “Worms Spur Call for Diversity.” *EWeek – Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=59124,00.asp (2 February 2004).

Carnegie Mellon University Software Engineering Institute. (1996). “Testimony of Richard Pethia Manager, Trustworthy Systems Program and CERT Coordination Center.” *1996 Congressional Hearings Intelligence and Security*. http://www.fas.org/irp/congress/1996_hr/s960605m.htm (3 February 2004).

Carnegie Mellon University Software Engineering Institute. (2003). “Before You Connect a New Computer to the Internet.” *CERT® Coordination Center*. http://www.cert.org/tech_tips/before_you_plug_in.html (30 December 2003).

Carr, David F. “Case 101 – A Dissection – U.N. Mission in Sierra Leone – On the Edge of Peace.” *Baseline Magazine* No. 26 (January 2004): pp. 32–52.

Carr, Jack, Mathewson, Frank, and Neil Quigley. 1995. Stability in the absence of deposit insurance: the Canadian banking system, 1890-1966. Journal of Money, Credit & Banking. Vol. 27, No. 4: 1137-59.

Carrier, Brian. (2002). Atstake Corporate White Paper. “Open Source Digital Forensics Tools: The Legal Argument.” pp. 1-11. http://www.atstake.com (30 December 2003).

Casey, James and Frances Picherack. (2003). *The Regulation of Complementary and Alternative Health Care Practitioners: Policy Considerations*. Health Systems Division-Health Canada http://www.hc-sc.gc.ca/hppb/healthcare/pubs/comp_alt/regs.html#t3 (12 February 2004).

CATA Alliance. (2004). “Cyber Security at the Top of CATA's Business Agenda.” http://www.cata.ca/Media_and_Events/Press_Releases/cata_pr02090401.html (10 February 2004).

CED Magic Web Site. (1981). “The IBM Personal Computer is Introduced.” *CED in the History of Media Technology*. http://www.cedmagic.com/history/ibm-pc-5150.html (1 March 2004).

Cerf, Vinton G. *et al*. (2003). “A Brief History of the Internet.” *Internet Histories*. http://www.isoc.org/internet/history/brief.shtml (19 February 2004).

Cerf, Vinton G. (2001). “A Brief History of the Internet and Related Networks.” *Internet Histories*. http://www.isoc.org/internet/history/cerf.shtml (19 February 2004).

Cerf, Vinton G. (1997). “Computer Networking: Global Infrastructure for the 21st Century.” *Computing Research Association*. http://www.cs.washington.edu/homes/lazowska/cra/networks.html (17 February 2004).

Chabrow, Eric. (2004). “GAO Faults 'Inconsistent' Online Security Programs.” *Information Week*. http://www.informationweek.com/shared/printableArticle.jhtml?articleID=17301563 (30 January 2004).

CICA – Accounting Standards Oversight Council. (2003). *Meeting the Challenge – Annual Report 2002-2003 of the Accounting Standards Oversight Council*. http://www.cica.ca/index.cfm/ci_id/15410/la_id/1.htm (2 March 2004).

Claburn, Thomas. (2004). “The Password Is: Liability.” *Information Week.* http://www.informationweek.com/shared/printableArticle.jhtml?articleID=18200511 (26 February 2004).

Clarke, Richard, and Lee Zeichner. (2004). “How To Protect Yourself Against Hackers.” *Internet Week*. http://interactiveage.com/security02/showArticle.jhtml?articleID=17200532 (8 January 2004).

CNN.com Staff. (2004). “Expert: Microsoft dominance poses security threat – Biology stirs software 'monoculture' debate.” http://www.cnn.com/2004/TECH/biztech/02/16/microsoft.monoculture.ap/index.html (17 February 2004).

Coffer, Walter, and Luces M. Faulkenberry. *Electrical Power Distribution and Transmission*. Englewood Cliffs: Prentice-Hall, Inc., 1996.

Cohen, Marjorie G. (2001). From public good to private exploitation: GATS and the restructuring of Canadian electrical utilities. Canadian-American Public Policy. Vol. 48: 1–79.

Collins, Tony. (2001). “Chinook pilots may have been unable to slow down, squadron leader tells Lords.” *Computer Weekly*. http://www.computerweekly.com/Article106950.htm (5 February 2004).

Collins, Tony. “Lives on the line?” *Computer Weekly* (27 July 1995): pp. 26–28.

Collins, Tony. (2001). “Lords vote to undertake limited Chinook inquiry.” *Computer Weekly*. http://www.computerweekly.com/Article101370.htm (5 February 2004).

Collins, Tony. (2002). “MoD refuses to concede error in Chinook verdict.” *Computer Weekly*. http://www.computerweekly.com/Article114442.htm (5 February 2004).

Collins, Tony. (2001). “RAF chiefs rubbish software claims.” *Computer Weekly*. http://www.computerweekly.com/articles/article.asp?liArticleID=108277&liArticleTypeID=1&liCategoryID=2&liChannelID=28&liFlavourID=1&sSearch=&nPage=1 (5 February 2004).

Collins, Tony. (2002). “Victory! Lords confirm CW stand – software flaw could have caused Chinook crash.” *Computer Weekly*. http://www.computerweekly.com/Article109778.htm (5 February 2004).

Compass Inc. (2002). “National Study of Academic Researchers.” http://www.ocipep.gc.ca/research/scie_tech/CI/climatechg/2002-D012_e.asp (30 December 2003).

Computer Hope Web Site. (2004). “Programming Definitions.” http://www.computerhope.com/jargon/program.htm (2 March 2004).

Computer Science and Telecommunications Board – National Research Council. (2002). *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*. http://www.cybersecure.ca/popl.pdf (23 January 2004).

Computer Weekly Staff. (2000). “Defence Minister misleads MPs over Chinook accident.” *Computer Weekly*. http://www.computerweekly.com/Article20211.htm (5 February 2004).

Computer Weekly Staff. (2002). “Lessons to be learned from Chinook tragedy.” *Computer Weekly*. http://www.computerweekly.com/Article109772.htm (5 February 2004).

Cooper, Charles. (2003). “Lock 'em up for substandard software.” http://zdnet.com.com/2100-1104_2-5129641.html (19 December 2003).

Cornish, Bill. (2001). “Wireless Devices and the New Security Challenges.” *CanCERT Bulletin* Vol. 4, No. 2 (August 2001): pp. 6–17 http://www.cancert.ca/Bulletins/CanCERT_Bulletin_Vol4_No2.pdf (9 March 2004).

Costa, J. Keith. (2001). “Concerned about threats to critical infrastructures...Canadian official calls for Cyber-Security Exercise with United States.” *Inside the Pentagon*. http://www.ocipep.gc.ca/whoweare/articles/article_ipent1_e.asp (30 December 2003).

Costa, J. Keith. (2002). “While reaching out to Washington, other allies…Canada forges ahead with master plan to guard key infrastructures.” *Inside the Pentagon*. (30 December 2003). http://www.ocipep.gc.ca/whoweare/articles/article_ipent2_e.asp

Coursey, David. (2004). “Why broadband over power lines is a bad idea.” *ZD Net Anchor Desk* http://reviews-zdnet.com.com/AnchorDesk/4630-7298_16-5123406.html?tag=print (3 March 2004).

Cox, Mark. (2004). “Customers still in dark about blackouts: Accenture study.” *ConnectIT* http://www.integratedmar.com/connectIT/story.cfm?item=367 (16 February 2004).

Crawford, C. Merle, C. Anthony Di Benedetto and Roger J. Calantone. *New products Management*. New York: Irwin McGraw-Hill, 2000.

Customer Relationship Management Research Center. (2004). http://www.cio.com/research/crm (28 February 2004).

Cusumano, Michael A. (2004). Who is Liable for Bugs and Security Flaws in Software? Communications of the ACM. Vol. 47, No. 3: 25–27.

D. Scott Campbell & Associates Inc., Lipchak, Andrew and McDonald, John. (2002). *A Case for Action for Information Management*. http://www.archives.ca/06/docs/action_e.pdf (23 January 2004).

Daly, Brian. “Experts say personal information, networks vulnerable as Internet grows.” *Canadian Press News Wire* (27 August 2002).

Daniels, Ron and Michael J. Trebilcock. (2000). Electricity Restructuring: The Ontario Experience. The Canadian Business Law Journal. Vol. 33, No. 2: 161–192.

Darby, Chris, Geer, Dr. Daniel, Germanow, Abner, and Chris Wysopal. (2002).“The Injustice of Insecure Software.” pp. 1-6. http://www.atstake.com (30 December 2003).

Darko, Anima. (2002). “Computer Aided Disaster.” http://www.ee.ualberta.ca/~musilek/cmpe510/Computer_Aided_Disaster.pdf (5 February 2004).

Darroch, James L. 1992. Global competitiveness and public policy: the case of Canadian multinational banks. Business History. Vol. 34, No.3: 153–176.

Darwinmag.com. (2002). “Service level Agreements.” *Darwin Magazine.* http://embedded.com/98/9805br.htm (9 February 2004).

Darwinmag.com. (2002). “Service level Agreements – Overview.” *Darwin Magazine.* http://guide.darwinmag.com/technology/outsourcing/sla/index.html?action=print (9 February 2004).

Davis, Tom. (2003). “2003 Federal Computer Security Report Card.” *Committee on Government Reform*. http://www.reform.house.gov/TIPRC/Hearings/EventSingle.aspx?EventID=652 (10 December 2003).

DeMarco, Tom and Timothy Lister eds. *Software State-of-the-Art: Selected Papers.* New York: Dorset House Publishing, 1990.

Devlin, Dennis. (2002). “Primum Non Nocere.” *Secure Business Quarterly*. Vol. 2, Issue 3. http://www.sbq.com (30 December 2003).

Digital Defence. (2002). “5 Charged In Child Porn Case.” *Information Security News 2002.* http://digitaldefence.ca/news/2002_020123.htm (26 February 2004).

Doss, David and William Yurcik. (2002). “CyberInsurance: A Market Solution to the Internet Security Market Failure.” In *Workshop on Economics and Information Security*, University of California, Berkeley May 2002. http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/53.pdf (3 February 2004).

Dowd, Kevin. 1994. Competitive banking, bankers' clubs and bank regulation. Journal of Money, Credit & Banking. Vol. 26, No. 2: 289–308.

Doyle, Chris. (1997). Self regulation and statutory regulation. Business Strategy Review. Vol. 8, No. 3: 35-43.

Duke Law and Technology Review. (2002). “Protecting the Homeland by Exemption: Why the Critical Infrastructure Information Act of 2002 will degrade the Freedom of Information Act.” http://www.law.duke.edu/journals/dltr/articles/2002dltr0018.html (30 December 2003).

Duncan, Jim. (2002). “Responsible Vulnerability Disclosure: Challenges for Vendors Whose Products Are Infrastructural.” *Secure Business Quarterly*. Vol. 2, Issue 3. http://www.sbq.com/sbq/vuln_disclosure/sbq_disclosure_vendor_challenges.pdf (29 January 2004).

Dutt, Robert. (2004). “MyDoom spawns another sequel.” http://www.integratedmar.com/connectit/story.cfm?item=355 (11 February 2004).

Dvorak, John C. (2004). “The Big One.” *Newsweek.* http://www.pcmag.com/article2/0,4149,1490702,00.asp (4 February 2004).

Easynet Group. (2004). *Investor Information Glossary*. http://www.easynet.com/investorinfo/investorinfo_glossary.asp (11 February 2004).

Evans, Bob. (2004). “Business Technology: Keep Apps Simple As Possible, No Simpler.” *Information Week.* http://www.informationweek.com/story/showArticle.jhtml?articleID=17700250 (17 February 2004).

EWeek-Enterprise News and Reviews Staff. (2004). “Linux & Open Source,” *EWeek-Enterprise News and Reviews.* http://www.eweek.com/category2/0,4148,1237915,00.asp (1 March 2004).

Evans, Mark. (2003). “Rogers Edges Toward Telephony War v. BCE ‘Prudent For Us’: Will Start Service Using Internet By 2005, Says CEO.” *National Post* http://www.vonage.com/corporate/press_news.php?PR=2003_12_10_1 (2 March 2004).

Fabian, Robert. (2004). “Should Software Professionals be licensed?” *IT World Canada*. http://www.itworld.com/Career/3710/040105itlicense/pfindex.html (8 January 2004).

Farber, Dan. (2003). “Massive software engineering reform a must.” http://techupdate.zdnet.com/techupdate/stories/main/Massive_software_engineering_reform_is_a_must.html (12 December 2003).

Fisher, Dennis. (2004). “IT Losing Ground in Virus Battle.” *EWeek-Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=117996,00.asp (2 February 2004).

Fisher, Dennis. (2004). “Newest Trojan: Disguised to Do Damage.” *EWeek-Enterprise News and Reviews*. http://www.eweek.com/article2/0,4149,1429886,00.asp (2 February 2004).

Fisher, Dennis. (2003). “Report: Windows' Dominance a Hindrance to Security.” *EWeek-Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=107975,00.asp (2 February 2004.)

Fisher, Dennis. (2004). “Security Maven Calls for Internet 'Disease Control' Agency.” *EWeek-Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=117881,00.asp (2 February 2004).

Fisher, Dennis. (2004). “Security Vendors Partner to Improve Threat Response Time.” *EWeek-Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=115726,00.asp (9 January 2004).

Fisher, Dennis. (2002). “Software Liability Gaining Attention.” *EWeek-Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=21030,00.asp (30 January 2004).

Fitzsimons, Adrian P., Levine, Marc H., and Joel G. Siegel. 1995. Comparability of accounting and auditing in NAFTA countries. The CPA Journal. Vol. 65, No. 5: 38–45.

Forno, Richard. (2004). “Anti-virus industry: white knight or black hat?” *The Register UK*. http://www.theregister.co.uk/content/55/35579.html (17 February 2004).

Foster, Ed. “It's time to act: let's require vendors to disclose known bugs and incompatibilities.” *InfoWorld* Vol. 18, No. 10 (4 March 1996): pp. 56–57.

Foster, Scott. (2004). “Agriculture group puts safe food tracking on the menu.” *IT Businesss.ca*. http://www.itbusiness.ca/index.asp?theaction=61&sid=54738# (9 February 2004).

Foster, Scott. (2003). “E-marketers unite to address spam debate.” *IT Businesss.ca.* http://www.itbusiness.ca/index.asp?theaction=61&lid=1&sid=53943 (17 February 2004).

Foster, Scott. (2004). “Industry on hold for CRTC VoIP decision.” *IT Businesss.ca.* http://www.itbusiness.ca/index.asp?theaction=61&lid=1&sid=54816 (17 February 2004).

Foster, Scott. (2003). “Virus victims weigh cyber-insurance options: insurance providers offer policies to cover corporate damage caused by worms such as Blaster.” *Computing Canada*. http://www.findarticles.com/m0CGC/19_29/108992880/p1/article.jhtml (27 February 2004).

Fratto, Mike. (2004). “The 2004 Security Survivor’s Guide.” *Internet Week*. http://www.internetweek.com/breakingNews/showArticle.jhtml?articleID=17100035 (6 January 2004).

Freedman, David F. “Smart Machines.” *Inc.* (15 November 1999): p. 180.

Fried, Ina. (2003). “Is bulked-up HP ready for battle?” http://zdnet.com.com/2102-1103_2-5116531.html?tag=printthis (10 December 2003).

Friedland, Martin L. (2002). “Notes for *The University of Toronto – A History*.” University of Toronto Press http://www.utppublishing.com/uoft_history/notes/notes_chapter39.pdf (4 March 2004).

Fyfe, Stephen and William McLean. (2002.) Opportunities for Municipally Owned Corporations in Ontario's Electricity Market. Canadian Tax Journal. Vol. 50, No. 3: 970–1010.

Gage, Debbie. (2004). “Should the Government Regulate Internet Security?” *Baseline Magazine.* http://www.baselinemag.com/print_article/0,1406,a=120340,00.asp (3 March 2004).

Gage, Debbie, and John McCormick. (2004). “Can Software Kill?” *EWeek-Enterprise News and Reviews.* http://www.eweek.com/print_article/0,1761,a=121063,00.asp (9 March 2004).

Gage, Debbie, and John McCormick. (2004). “We Did Nothing Wrong.” *Baseline Magazine.* http://www.baselinemag.com/print_article/0,1406,a=121048,00.asp (11 March 2004).

Galli, Peter. (2004). “Novell to Offer Linux Indemnification Program.” *EWeek-Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=116219,00.asp (13 January 2004).

Ganssle, Jack. (1998). “Disaster.” *Break Points*. http://embedded.com/98/9805br.htm (9 February 2004).

Geer, Dan *et al*. (2003).“Cyber*In*security: The Cost of Monopoly – How the Dominance of Microsoft’s Products Poses a Risk to Security.” *Computer & Communications Industry Association*. http://www.ccianet.org/papers/cyberinsecurity.pdf (28 February 2004).

Geer Jr., Dr. Daniel E. (2002). “What is Vulnerability Disclosure?” *Secure Business Quarterly*. Vol. 2, Issue 3. http://www.sbq.com (30 December 2003).

Ghosh, Anup K. and Michael J. Del Rosso. (1999). “The Role of Private Industry and Government in Critical Infrastructure Assurance.” http://www.isi.edu/gost/cctws/delroso-ghosh.PDF (3 February 2004).

Gibbs, Nancy. “Lights Out: First the good news: the biggest blackout ever in North America brought out the best in millions of citizens. Now the bad: it exposed a woefully fragile electrical system. How did it happen? And how vulnerable are we to another shutdown?” *Time* Vol. 162, No. 8 (25 August 2003): pp. 30–36.

Gilbertson Davis Emerson LLP. (2000). *Nostradamus' Strategy For Millennium Bug Litigation:"I Told You So."* http://www.gilbertsondavis.com/publications/nostra_strategy.htm (2 March 2004).

Goodwins, Rupert. (2004). “Software lessons from Mars.” *News Commentary*. http://zdnet.com.com/2102-1107_2-5148988.html?tag=printthis (29 January 2004).

Greiner, Lynn. “Demand more accountability from vendors.” *Computing Canada* Vol. 24, No. 47 (14 December 1998): pp. 17-19.

Gross, Grant. (2003). “Gov’t agency uses buying power to encourage security.” http://www.infoworld.com/article/03/09/23/Hngovbuying_1.html (30 December 2003).

Hachman, Mark. (2004). “RSA Panel: Cryptography Can't Foil Human Weakness.” *EWeek-Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=120168,00.asp (25 February 2004).

Hamilton, Tyler. (2004). “Music Groups Appeal Copyright Ruling.” *The Toronto Star*. http://www.thestar.ca/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1074035410130&call_pageid=970599109774&col=Columnist971715454851 (15 January 2004).

Handa, Sunny, Johnston, David and Charles Morgan. *Cyberlaw –W hat You Need to Know about Doing Business Online*. Toronto: Stoddart Publishing Co., 1997.

Hardin, Garrett. (1968). “The Tragedy of the Commons.” *Science* 162 (1968): 1243–1248. http://www.dieoff.com/page95.htm (19 February 2004).

Harlick, James E. Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). “Canadian Information Technology Security Symposium.” http://www.ocipep.gc.ca/whoweare/speeches/jh_cits_e.asp (30 December 2003).

Hasan, Ragib. (2002). “History of Linux.” *Department of Computer Science University of Illinois at Urbana-Champaign*. https://netfiles.uiuc.edu/rhasan/linux/ (1 March 2004).

Health Canada. (2002). “Limits of Human Exposure to Radiofrequency Electromagnetic Fields in the Frequency Range from 3 KHz to 300 GHz – Safety Code 6.” *Consumer and Clinical Radiation Protection.* http://www.hc-sc.gc.ca/hecs-sesc/ccrpb/publication/99ehd237/chapter1.htm (9 March 2004).

Health Professions Regulatory Advisory Council. (1999). *Weighing the Balance – A Review of the Regulated Health Professions Act – Request for Submissions*. http://www.hprac.org/downloads//fyr/weighing.pdf (13 February 2004).

Heckman, Carey. (2003). “Two Views on Security Software Liability: Using the Right Legal Tools.” *IEEE Security & Privacy*. Vol. 1, No. 1 (January/February 2003): pp. 73–75. http://csdl2.computer.org/dl/mags/sp/2003/01/j1073.htm (24 February 2004).

Help Desk Solutions. (1999). “Changes in the Customer Support Industry.” *Computer News.* http://www.helpdesksolutions.com/Publications/change_support.htm (27 February 2004).

Hewitt, Michael. “FYI: Recent Canadian decisions on accountants’ liability (1997-2001).” *Beyond Numbers* (1 October 2002): pp. 28–32.

Hobby, Jason. “See you in court.” *Computer Weekly* (26 October 1995): pp60–62.

Hoffman, Steve. 1996. Enhancing power grid reliability. EPRI Journal. Vol. 21, No.6: 6–15.

Holloway, Derek. (1992). “Liability Implications of CADD.” *Loss Control Information – Architects and Engineers.* Bulletin 91 (January 1992). http://www.encon.ca/english/lcb/bulletins/display.cfm?ID=29 (9 February 2004).

House of Representatives. (2002). *Cyber Security Research and Development Act*. http://www.house.gov/science/hot/cyber/cyberfile.pdf (29 January 2004).

Howe, Walt. (2004). *Walt’s Internet Glossary - Glossary of Internet Terms*. http://www.walthowe.com/glossary/n.html (22 February 2004).

Hrab, Roy and Michael J. Trebilcock. (2003). What will keep the lights on in Ontario: responses to a policy short-circuit. C.D. Howe Institute Commentary. 191–220.

Huber, Peter, and Mark Mills. “Brawn & Brains.” *Forbes* Vol. 172, No. 5 (15 September 2003): pp: 46–48.

Hulme, George V. (2004). “Application Security Standard Edges Forward.” *Internet Week.* http://www.internetweek.com/shared/printableArticle.jhtml?articleID=18100224 (24 February 2004).

Hulme, George V. (2004). “Security Threats Won't Let Up This Year.” *Internet Week.* http://www.internetweek.com/shared/printableArticle.jhtml?articleID=17200253 (8 January 2004).

Hulme, George V. (2003). “Spending To Fend Off Online Attacks Grows In 2004.” *Information Week*. http://www.informationweek.com/story/showArticle.jhtml;jsessionid=OO0GE5JL5WV1KQSNDBCSKHQ?articleID=17100128 (29 December 2003).

Huuhtanen, Matti. (2004). “'Mydoom' Creators Start Up 'Doomjuice'” http://apnews.myway.com/article/20040210/D80KGV5O0.html (11 February 2004).

Hyder, Elaine B. et al. (2002). “eSourcing Capability Model () for IT-enabled Service Providers v1.1.” *CMU-CS-02-155 – Computer Science Department – School of Computer Science – Carnegie Mellon University*. http://itsqc.srv.cs.cmu.edu/escm/documents/eSCM_Model_1.1.pdf (11 February 2004).

Iacobucci, Edward, Trebilcock, Michael J., and Ralph A. Winter. (2003). “Economic Deregulation of Network Industries Managing the Transition to Sustainable Competition.” http://128.100.167.70/pages/DEREGULATION_MAY%2015%202003.doc. (16 February 2004).

IBM Corp. (2004). “Linux at IBM,” http://www-1.ibm.com/linux/ (27 February 2004).

IBM Corp. (2004). *IBM Deep Computing Institute*. http://www.research.ibm.com/dci/cat4_domain.shtml (5 March 2004).

ICB Toll Free News. (2000). “Dot Com Wars.” http://icbtollfree.com/article.cfm?articleId=1399 (3 February 2004).

IEEE Computer Society. (2004). “History of the Joint IEEE Computer Society and ACM Steering Committee for the Establishment of Software Engineering as a Profession.” http://www.computer.org/tab/seprof/history.htm (28 February 2004).

Ihnatko, Andy. “Right-protected software.” *MacUser* Vol. 9, No. 3 (March 1993): pp. 29–34.

Industry Canada. (1999). “RSS-102 – Evaluation Procedure for Mobile and Portable Radio Transmitters with respect to Health Canada's Safety Code 6 for Exposure of Humans to Radio Frequency Fields.” *Spectrum Management and Telecommunications Policy – Radio Standards Specification*. http://strategis.ic.gc.ca/epic/internet/insmt-gst.nsf/vwapj/rss102.pdf/$FILE/rss102.pdf (9 March 2004).

Industry Canada. (2004). “Digital Apparatus.” *Spectrum Management and Telecommunications Policy – Interference-Causing Equipment Standard*. http://strategis.ic.gc.ca/epic/internet/insmtgst.nsf/vwapj/ices003e.pdf/$FILE/ices003e.pdf (9 March 2004).

Industry Canada. (2004). "RSS-192 - Fixed Wireless Access Equipment Operating in the Band 3450–3650 MHz." *Spectrum Management and Telecommunications Policy – Radio Standards Specification*. http://strategis.ic.gc.ca/epic/internet/insmt-gst.nsf/vwapj/rss192e.pdf/$FILE/rss192e.pdf (9 March 2004).

Industry Canada. (2004). "RSS-195 - Wireless Communications Service Equipment Operating in the Bands 2305-2320 MHz and 2345-2360 MHz." *Spectrum Management and Telecommunications Policy – Radio Standards Specification*. http://strategis.ic.gc.ca/epic/internet/insmtgst.nsf/vwapj/rss195e_dec30.pdf/$FILE/rss195e_dec30.pdf (9 March 2004).

InfoSec Research Council. (1999). "National Scale INFOSEC Research Hard Problems List."http://www.infosec-research.org/docs_public/IRC-HPL-as-released-990921.doc (9 February 2004).

Institute for Information Infrastructure Protection. (2002). *National Information Infrastructure Protection – Research and Development Agenda Initiative Report – Information InfrastructureProtection: Survey of Related Roadmaps and R &D Agendas.* http://www.thei3p.org/documents/analyses/I3P_Roadmap_Analysis_V1.0s.pdf (10 March 2004).

INTEL Corp. (2002). "Expanding Moore's Law – The Exponential Opportunity" *Intel Technology Update* (Fall, 2002) ftp://download.intel.com/labs/eml/download/EML_opportunity.pdf (2 March 2004).

INTEL Corp. (2002). "Moore's Law". http://www.intel.com/research/silicon/mooreslaw.htm (28 February 2004).

Isenberg, Doug. (2004). "Unexpected twists in Internet law" http://zdnet.com.com/2100-1107_2-5134877.html (6 January 2004).

IT Cortex. (2004). "Failure Rate." http://www.it-cortex.com/Stat_Failure_Rate.htm (27 February 2004).

IT Disaster Recovery Planning. (2003). *Ensuring Business Continuity with Effective Asset Availability Management Conference*. http://www.drie.org/documents/ITDRP.pdf (30 December 2003).

IT World.com. (2001). "10 myths about service-level agreements." http://www.itworld.com/Man/2679/ITW010427sla/ (9 February 2004).

Jackson, William. "Frustrated lawmakers prod justice, vendors for accountability in worm and virus crimes." *Government Computer News* Vol. 22, No. 28 (22 September 2003): pp. 13–14.

Jackson, William. “IT, power grids not primary terror targets, FBI says.” *Government Computer News* Vol. 22, No. 27 (15 September 2003): pp. 12–13.

Jacquith, Andrew. (2002). Atstake Corporate White Paper. “The Security of Applications: Not all are Created Equal.” pp. 1–12. http://www.atstake.com (30 December 2003).

Jerome, Marty. “Software Safeguards.” *PC/Computing* Vol. 3, No. 2 (February 1990): pp. 119–121.

Jesdanun, Anick. (2004). “GE Energy acknowledges blackout bug.” *The Associated Press* http://www.securityfocus.com/printable/news/8032 (16 February 2004).

Jesper / Laisen / DK. (2001). “Hack, Hackers, and Hacking.” http://www.laisen.dk/Hack__Hackers__and_H.1233.0.html (5 March 2004).

Johnson, R. Colin. “Power-grid planners plug in to neuro-fuzzy.” *Electronic Engineering Times* (27 September 1999): pp. 73–74.

Joyce, Ed. “Software bugs: a matter of life and liability”. *Datamation* Vol. 33, No. 10 (15 May 1987): pp. 88–97.

Kadlec, R.E. (1993). Winds of change in utility regulation. Canadian Business Review. Vol. 20, No. 4: 39–42.

Kahney, Leander. (2003). “Fast Track for Science Data.” *Wired News*. http://www.wired.com/news/print/0,1294,61102,00.html (17 November 2003).

Kane, Edward J. 1996. De jure interstate banking: why only now? Journal of Money, Credit & Banking. Vol. 11, No. 2: 141–161.

Kanellos, Michael. (2004). “Is security getting any easier?” *CNET News.com*. http://zdnet.com.com/2102-1105_2-5164431.html?tag=printthis (25 February 2004).

Kaner, Cem. (1999). “The Future of Software Liability.” *Cem Kaner Testing Computer Software Conference June 1999*. http://www.kaner.com/pdfs/uspdi_keynote.pdf (30 January 2004).

Kaner, Cem. (2000). “Why You Should Oppose UCITA.” http://www.badsoftware.com/claw2000.htm (4 February 2004).

Keizer, Greg. (2003). “Phishing Attacks Soar.” *Internet Week*. http://www.internetweek.com/shared/printableArticle.jhtml?articleID=17100208 (6 January 2004).

Keizer, Greg. (2003). “Security: From Bad to Worse?” *Information Week*. http://www.informationweek.com/shared/printableArticle.jhtml?articleID=17100254 (5 January 2004).

Kenneally, Erin. (2001). “Stepping on the digital scale - Duty and Liability for Negligent Internet Security.” *;login: The Magazine of USENIX & SAGE*. Vol. 26, No. 8 (December 2001): pp. 62–77. http://www.usenix.org/publications/login/2001-12/pdfs/kenneally.pdf (24 February 2004).

Kenneally, Erin. (2002). “Who’s Liable for Insecure Networks?” *IEEE Security & Privacy*. Vol. 35, No. 6 (June 2002): pp. 93–95. http://csdl2.computer.org/dl/mags/co/2002/06/r6093.htm (24 February 2004).

King, Michael C. “An Introduction to the Health Professions Act.” Calgary Regional Health Authority. http://www.calgaryhealthregion.ca/clin/adultpsy/articles/hpa2.pdf. (4 February 2004).

Kleinrock, Leonard. “Information Flow in Large Communication Nets.” *RLE Quarterly Progress Report* (July 1961).

Koerner, Brendan I. “Bugging Out - Is your software screwing up? Tough.” *The New Republic* (27 November 2000): pp. 13–15.

Krebs, Brian. (2003). “Gov’t Computer Security Lagging – Report.” *The Washington Post*. http://www.washingtonpost.com/ac2/wp-dyn/A49030-2003Dec9?language=printer (10 December 2003).

Labaton, Stephen. (2004). “F.C.C. Begins Rewriting Rules on Delivery of the Internet.” *The New York Times on the Web*. http://www.nytimes.com/2004/02/12/technology/12CND-NET.html?ex=1077682218&ei=1&en=7d5a82c84583aff0 (23 February 2004).

Law Society of Upper Canada. (2003). *Emerging Issues Committee – Report to Convocation* (26 June 2003). http://www.lsuc.on.ca/news/pdf/convjune03_emergingissues.pdf (4 February 2004).

Leech, John. (2002). “Our Shared Responsibility: Interview with Margaret Purdy.” *Canadian Government Executive Magazine*. http://www.ocipep.gc.ca/whoweare/articles/article_ipent3_e.asp (30 December 2003).

Lemos, Robert. (2003). “A two-pronged approach to cybersecurity.” *The Washington Post*. http://www.washingtonpost.com/ac2/wp-dyn/A49030-2003Dec9?language=printer (3 December 2003).

Lemos, Robert. (2003). “Bush unveils final cybersecurity plan.” http://zdnet.com.com/2102-1105_2-984697.html?tag=printthis (10 December 2003).

Lemos, Robert. (2003). “Feds get a ‘D’ in computer security.” http://zdnet.com.com/2102-1105_2-5118344.html?tag=printthis (10 December 2003).

Lemos, Robert. (2004). “Government planning cyberalert system.” *CNET News.com* http://news.com.com/2102-7348_3-5148708.html?tag=st_util_print (29 January 2004).

Lemos, Robert. (2003). “Report: Microsoft dominance poses security risk.” http://zdnet.com.com/2102-1105_2-5081214.html?tag=printthis (29 January 2004).

Lemos, Robert. (2004). “Security a work in progress for Microsoft.” http://zdnet.com.com/2102-1105_2-5141765.html (16 January 2004).

Lemos, Robert. (2004). “Tracking the seeds of destruction.” http://zdnet.com.com/2102-1105_2-5140991.html (16 January 2004).

Lemos, Robert, and Declan McCullagh. (2002). “Cybersecurity plan lacks muscle.” http://zdnet.com.com/2100-1105-958545.html?tag=nl (10 December 2003).

Leveson, Nancy G. 1991. Software safety in embedded computer systems. Communications of the ACM. Vol. 34, No. 2: 34–45.

Leyden, John. (2004). “Flaw on Tuesday, exploit by Monday.” *The Register UK*. http://www.theregister.co.uk/content/55/35592.html (17 February 2004).

Leyden, John. (2004). “Windows source code exploit released.” *The Register UK*. http://www.theregister.co.uk/content/55/35611.html (17 February 2004).

Lewis, Ted G. and Paul W. Oman eds. *Milestones in Software Evolution* Los Angeles: IEEE Computer Society Press, 1990.

Linden, Allen M. *Canadian Tort Law*, 5th ed. Toronto: Butterworths, 1993.

Lohr, Steve. (2003). “Product Liability Lawsuits Are New Threat to Microsoft.” *The New York Times.* http://www.lexisone.com/news/n100603a.html (2 March 2004).

Lowenstein, Frank. “Software Liability.” *Technology Review* Vol. 90 (January 1987): pp. 9–10.

Madar, Daniel. 2002. Rail mergers, trade, and federal regulation in the United States and Canada. Publius. Vol.32, No. 1: 143–159.

Mann, Charles C. (2002). “Why software is so bad ... ... and what's being done to fix it.” *MSNBC Technology and Science.* http://www.cs.queensu.ca/~dingel/whySWIsSoBad.pdf (5 March 2004).

Marron, Keith. (2003). “New audit rules count for IT departments.” *The Globe and Mail*. http://www.globetechnology.com/servlet/story/RTGAM.20031210.wsarb1210/BNPrint?Technology/?main (11 December 2003).

Matthews, Ian. (2003). "The Amazing Commodore PET." *Commodore Business Machines Product Line Up*. http://www.commodore.ca/products/pet/commodore_pet.htm (22 February 2003).

McCullagh, Declan. (2004). "New security law sacrifices privacy." *CNET News.* http://zdnet.com.com/2100-1107-5155462.html?tag=sas.email (10 February 2004).

McFadden, David. "Power to the people: The opening of Ontario's electricity market is not just a Get-rich scheme for a greedy few. It will benefit the economy, the environment and Consumers." *Financial Post* (*National Post*) (2 May 2002): FP 15.

McGeary, Johanna. "An Invitation To Terrorists?" *Time* Vol. 162, No. 8 (25 August 2003): p. 38.

McGraw, Gary and Greg Morrisett. (2000). "Attacking Malicious Code: A Report to the Infosec Research Council." *IEEE Software.* (September-October 2000): pp. 33–41 http://www.infosec-research.org/docs_public/ISTSG-MC-report.pdf (10 March 2004).

Mead, Nancy R. (2003). "International Liability Issues for Software Quality." *CERT Research Center Special Report CMU/SEI-2003-SR-001*. http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03sr001.pdf (24 February 2004).

Mears, Jennifer. (2004). "SCO renews threats; Novell offers indemnification." *Network World Fusion.* http://www.nwfusion.com/news/2004/0119linuxidem.html (2 March 2004).

MEMS and Nanotechnology Clearinghouse. (2004). "What is MEMS Technology?" http://www.memsnet.org/mems/what-is.html (February 23, 2004).

Meyer, Gabriel S, Raul, Alan Charles, and Frank R. Volpe. (2001). "Liability for Computer Glitches and Online Security Lapses." *BNA Electronic Commerce Law Report* Vol. 6, No. 31 (8 August 2001): 849 http://www.sidley.com/cyberlaw/features/liability.asp (27 February 2004).

Moffina, Rick and Mike Blanchfield. "Canada's cyber network, pipelines and power grids, which are all tied to the United States, are the most likely targets of terrorists." *CanWest News* (21 December 1999): pp. 1–3.

Moore, Gordon E. (1965). "Cramming more components onto integrated circuits." *Electronics* Vol.38, No. 8 (19 April 1965). ftp://download.intel.com/research/silicon/moorespaper.pdf (1 March 2004).

Morgan, Brian. "New Liabilities." *CA Magazine* Vol. 136, No. 5 (1 June 2003): pp. 34–36.

Morrissey, Jane. "Lawmakers to Consumers: Tough Luck!" *PC World* Vol. 16, No. 10 (October 1998): p.70.

Mucklestone, Connie. (2001). “Strategic Plan Vision sparks lively discussion.” *March 26, 2001 meeting: Professional Engineers Ontario.* http://www.peo.on.ca/publications/DIMENSIONS/mayjune2001/MJ01InCouncil.pdf (1 March 2004).

Mueller, Milton. 1999. ICANN and Internet Regulation. Communications of the ACM. Vol. 42, No. 6: 41–45.

Munro, Jay. (2004). “Beating the New MyDoom (Windows) Variant.” *EWeek-Enterprise News and Reviews*. http://www.pcmag.com/print_article/0,3048,a=117754,00.asp (2 February 2004).

Myers, Edith. “End to as-is sales? Buyers want more protection, but the last thing vendors want are laws that say they must provide warranties with their products”. *Datamation* Vol. 31 (15 September 1985): pp. 68–70.

National Infrastructure Protection Center. (2002). *Risk Management: An Essential Guide to Protecting Critical Assets*. November 2002. http://www.nipc.gov/publications/nipcpub/P-Risk%20Management.pdf (28 December 2003).

Natkin, Kenneth H. 1994. Legal risks of design/build. Architecture. Vol. 83, No. 9: 125–129.

Neumann, Peter G. (1997). “Computer Security in Aviation: Vulnerabilities, Threats, and Risks.” *International Conference on Aviation Safety and Security in the 21st Century – White House Commission on Safety and Security, and George Washington University* http://www.gwu.edu/~cms/aviation/track_ii/neumann.html (12 February 2004).

Newton, John. (2003). “Federal Legislation for Disaster Mitigation: A Comparative Assessment between Canada and the United States.” http://www.ocipep.gc.ca/research/scie_tech/disMit/en_mitigat/1995_D014_e.asp (30 December 2003).

Nissenbaum, Helen. 1994. Computing and accountability. Communications of the ACM (Association for Computing Machinery). Vol. 37, No. 1: 72–81.

Norman, John. (2004). “Ontario’s electricity dilemma: crisis or opportunity?” *The Varsity.* http://www.thevarsity.ca/global_user_element?printpage.cfm?storyid=598305 (12 February 2004).

Nulty, Peter, and Edward Prewitt. “Utilities flirt with Adam Smith; respected utility executive are demanding greater freedom to buy, make, and transmit power.” *Time* Vol. 117, No. 12 (6 June 1988): pp. 173–178.

O'Neil, Michael. 2001. Cybercrime Dilemma. Brookings Review. Vol. 19, No. 1: 28–35.

OneStat.com. (2002). “Microsoft’s Windows OS global market share is more than 97% according to OneStat.com.” http://www.onestat.com/html/aboutus_pressbox10.html (4 March 2004).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). “About Critical Infrastructure Protection.” http://www.ocipep.gc.ca/critical/index_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). *An Assessment of Canada’s National Critical Infrastructure Sectors*. http://www.ocipep.gc.ca (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). “Disaster Mitigation.” http://www.ocipep.gc.ca/NDMS/consult_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2002). *DRAFT – Tool to Assist Owners and Operators to Identify Critical Infrastructure Assets*. http://www.ocipep.gc.ca (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2001). “Emergency Preparedness Digest – Back Issues.” http://www.ocipep.gc.ca/ep/ep_digest/js_2001_feal_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). “Federal Emergency Preparedness in Canada.” http://www.ocipep.gc.ca/info_pro/fact_sheets/general/backgd_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). “International Consortium Releases List of the Top Twenty Internet Security Vulnerabilities.” http://www.ocipep.gc.ca/info_pro/NewsReleases/NR/2003/NR03-0810_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). “Legislation – Emergency Preparedness in Alberta.” http://www.ocipep.gc.ca/ep/legisla/ep_ab/e_p_p_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). “Microsoft SQL 2000 “Slammer” Worm – Impact Paper.” pp. 1–13. http://www.ocipep.gc.ca (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). “National Critical Infrastructure Assurance Program.” http://www.ocipep.gc.ca/info_pro/fact_sheets/general/CIP_NCIAP_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2002). "National Critical Infrastructure Assurance Program Discussion Paper." http://www.ocipep.gc.ca/critical/nciap/disc_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). "National Critical Infrastructure Assurance – The Case for Action." http://www.ocipep.gc.ca/critical/nciap/synopsis_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). "Search the Database." http://www.ocipep.gc.ca/disaster/search.asp?lang=eng. (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). "The Government Emergency Operations Coordination Centre (GEOCC)." http://www.ocipep.gc.ca/info_pro/fact_sheets/general/EM_gov_em_op_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness (2003). "Threats to Canada's Critical Infrastructure." pp.1–59. http://www.ocipep.gc.ca (30 December 2003).

Oracle Corp. (2004). Oracle Web Site. http://www.oracle.com/ (4 March 2004).

Parnas, David L. 1990. Evaluation of safety-critical software. Communications of the ACM. Vol. 33, No. 6: 636–648.

Parsons, Patrick. 2003. The evolution of the cables-satellite distribution system. Journal of Broadcasting & Electronic Media. Vol. 47, No. 1: 1–16.

Patterson, Cynthia A. and Stewart D. Personick, eds. (2003). *Critical Information Infrastructure Protection and the Law - An Overview of Key Issues.* Washington, D.C.: The National Academies Press, 2003. http://books.nap.edu/catalog/10685.html (19 February 2004).

PC Magazine Staff. "Unintended Consequences – Blackouts and Worms." (18 August 2003).

PC Week Staff. "Better software and guarantees – Now. Complaints about Windows 98 raise questions about software quality control and vendor accountability." *PC Week* Vol. 15, No. 29 (20 July 1998): pp. 29–30.

Pelline, Jeff. (2004). "MyDoom downs SCO site." *CNET News.* http://zdnet.com.com/2102-1105_2-5151572.html?tag=printthis (2 February 2004).

Perks, Gord. (2004). "Revenge of the nerds." *Eye Weekly.* http://www.eye.net/eye/issue/print.asp?issue_02.19.04/city/enviro.html (19 February 2004).

Phillips, Douglas E. 1994. When software fails: emerging standards of vendor liability under the Uniform Commercial Code. Business Lawyer. Vol. 50, No. 1: 151–181.

Phipps, Steven. 2001. "Order Out of Chaos:" A Reexamination of the Historical Basis for the Scarcity of Channels Concept. Journal of Broadcasting & Electronic Media. Vol. 45, No. 1: 57–80.

Picarille, Lisa. “License law may limit liability.” *Computerworld* Vol. 31, No. 19 (12 May 1997): pp. 1–2.

Pink Elephant Inc. (2003). “The Benefits of ITIL White Paper.” http://www.pinkelephant.com/pdf/Benefits_of_ITIL.pdf (9 February 2004).

Pink Elephant Inc. (2003). “The ITIL Story.” http://www.pinkelephant.com/pdf/The_ITIL_Story.pdf (9 February 2004).

Poulsen, Kevin. (2004). “Gates 'optimistic' on security.” *SecurityFocus* http://www.securityfocus.com/printable/news/8111 (25 February 2004).

Poulsen, Kevin. (2003). “Slammer worm crashed Ohio nuke plant network.” *SecurityFocus* http://www.securityfocus.com/printable/news/6767 (16 February 2004).

Poulsen, Kevin. (2004). “Software Bug Contributed to Blackout.” *SecurityFocus* http://www.securityfocus.com/printable/news/8016 (16 February 2004).

Poulsen, Kevin. (2003). “Sparks over Power Grid Cybersecurity.” *SecurityFocus* http://www.securityfocus.com/printable/news/3871 (16 February 2004).

Protti, Raymond J. (2002). “Banking On Both Sides of the 49th Parallel: Addressing the Regulatory and Legislative Demands of an Integrated Market.” *Canadian Banker Magazine*. (January 2002). http://www.cba.ca/en/magazine/getArticle.asp?at_id=203&pm=true (11 February 2004).

Protti, Raymond J. (2002). “National Regulation: Time to Get On with the Job.” *Canadian Banker Magazine*. (January 2002). http://www.cba.ca/en/magazine/getArticle.asp?at_id=202&pm=true (11 February 2004).

Red Hat Inc. (2004). *About Red Hat – The Open Source Leader*. http://www.redhat.com/ (28 February 2004).

Reuters. (2003). “U.N. confab to see tussle over Net control.” http://zdnet.com.com/2100-1104_2-5113744.html (10 December 2003).

Ricadela, Aaron. (2001). “The State of Software Quality.” *Information Week* http://www.informationweek.com/838/quality.htm (12 February 2004).

Rogerson, Professor Simon. (2002). “The Chinook Helicopter Disaster.” (Originally published As ETHIcol in the IMIS Journal. Vol 12, No. 2 (April 2002). http://www.ccsr.cse.dmu.ac.uk/resources/general/ethicol/Ecv12no2.pdf (10 February 2004).

Rooney, Paula. (2004). “OSDL, IBM, Intel Launch SCO Legal Defense Fund For Users.” *Internet Week*. http://www.internetweek.com/shared/printableArticle.jhtml?articleID=17300517 (15 January 2004).

Rosch, W.C. “Are You Protected from Software Publishers' Slip-Ups?” *P.C. Week* Vol. 2, No. 3 (22 January 1985): pp. 28–29.

Rosch, W.L. “Reading Between The Lines: Software Warranties”. *P.C. Week* Vol. 1, No. 45 (13 November 1984): pp. 121–124.

Rosenbaum, Joseph. (2004). “Protect Thyself 101: A primer on indemnification.” *ZD Net Tech Update*. http://techupdate.zdnet.com/techupdate/stories/main/indemnification_primer_print.html (2 March 2004).

Rosencrance, Linda. (2003). “Hacker breaks into U.S. e-voting firm’s site.” *IT World Canada*. http://www.itworld.ca/Pages/Docbase/ViewArticle.aspx?ID=idgml-1a7072b3-a1bf-4d64-a099-caecde7c7a85 (6 January 2004).

Ruby, Daniel. “Who's responsible for the bugs?” *PC Week* Vol. 23, No. 1 (27 May 1986): pp. 51–57.

Sager, Ira. “The View from IBM.” *Business Week* (30 October 1995), http://www.businessweek.com/1995/44/b34481.htm (28 February 2004).

Salesforce.com. (2004). “Salesforce.com.” http://www.salesforce.com/ (4 March 2004).

Sam Palmisano Presentation Transcript. (2003). *IBM Business Leadership Forum – San Francisco* (12 November 2003) http://www.ibm.com/ibm/sjp/11-12-2003.shtml (26 February 2004).

Sammet, Jean E. *Programming Languages: History and Fundamentals* Englewood Cliffs: Prentice-Hall, 1969.

Samuelson, Pamela. 1993. Communications of the ACM (Association for Computing Machinery). Vol. 36, No. 1: 21–29.

SANS. (2003). “The Twenty Most Critical Internet Security Vulnerabilities (Updated) – the Experts Consensus.” http://www.sans.org/top20/. (30 December 2003).

Saydjari, O. Sami. (2004). Cyber Defense: Art to Science. Communications of the ACM. Vol. 47, No. 3: 53–57.

Scheier, Robert L. “Lock the damned door!” *Computerworld* Vol. 31, No. 6 (10 February 1997): pp. 66–69.

Schick, Shane. (2004). “How the downloading debate is starting to affect other areas of IT.” *IT Business*.ca. http://www.itbusiness.ca/index.asp?theaction=61&sid=54933 (3 March 2004).

Schick, Shane. (2004). “Them’s the rules.” *IT Business*.ca. http://www.itbusiness.ca/print.asp?sid=54728 (5 February 2004).

Schiller, Jeffrey. (2002). “Response Vulnerability handling: ‘A Hard Problem’.” *Secure Business Quarterly*. Vol. 2, Issue 3. http://www.sbq.com/sbq/vuln_disclosure/sbq_disclosure_hard_problem.pdf (29 January 2004).

Schneier, Bruce. (2003). “Did Blaster cause the blackout?” http://zdnet.com.com/2102-1107_2-5118123.html?tag=printthis (9 December 2003).

Schneier, Bruce. (2002). “Fixing Network Security by Hacking the Business Climate.” www.counterpane.com/presentation4.pdf (19 January 2004).

Schneier, Bruce. (New unpublished introduction for previously published book). *Secrets & Lies Digital Security in a Networked World*. New York: John Wiley & Sons, 2000.

Schneier, Bruce. (2004). “Total surveillance becoming reality.” http://zdnet.com.com/2100-1107-5150608.html?tag=sas.email (3 February 2003).

Schoonmaker, Jim. (2004). “Security will ride shotgun with data in 2004.” http://zdnet.com.com/2102-1107_2-5149942.html?tag=printthis (29 January 2004).

SearchCIO.com. (2004). “Sarbanes-Oxley Act. http://searchcio.techtarget.com/sDefinition/0,,sid19_gci920030,00.html (17 February 2004).

Seltzer, Larry. (2003). “Is Computer Monoculture The Way Of The World?” *EWeek-Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=108093,00.asp (2 February 2004).

Shankland, Stephen. (2004). “Red Hat offers software warranty.” http://zdnet.com.com/2102-1104_2-5143326.html (21 January 2004).

Siklos, Pierre L. *Money, Banking and Financial Institutions – Canada in the Global Environment*. 2d ed. (Toronto: McGraw Hill Ryerson Limited, 1997.

Sikora, Vincent A. 2001. Public Agencies--Authority and Responsibilities. Journal of Environmental Health. Vol. 64, No. 1: 39.

Slofstra, Martin. “In conversation.” (Interview with Daniel Cooper, computer law expert-partner in McCarthy Tetrault of Toronto). *Computing Canada* Vol. 16, No. 8 (12 April 1990): pp. 13–17.

Soat, John. (2003). “Cybersecurity Starts at Home(land).” *Information Week*. http://www.informationweek.com/story/showArticle.jhtml?articleID=16600192 (9 December 2003).

Stamp, Mark. 2004. Risks of Monoculture. Communications of the ACM. Vol. 47, No. 3: 120.

Starr, Paul. 2003. A license for power. The American Prospect. Vol. 14, No. 5: 21–22.

Statistics Canada. (2002). *North American Industry Classification (NAICS) 2002*. http://stds.statcan.ca/english/naics/2002/naics02-class-search.asp?criteria=813910 (8 February 2004).

Statistics Canada. (2003). “The computer industry.” *Data and Computer*. http://www.statcan.ca/english/edu/power/ch4/industry/computers3.htm (24 February 2004).

Sun Microsystems, Inc. (2004). Internet Engineering group of Solaris Software http://playground.sun.com/pub/ipng/html/ipng-main.html (2 March 2004).

Surmacz, John. (2004). “Why Software Quality Still Stinks.” *IT World Canada*. http://www.itworld.ca/Pages/Docbase/ViewArticle.aspx?ID=idgml-a7a11aa5-b6fa-4ad7-a9ef-d53b6acc01d1 (8 January 2004).

Sutton, Neil. (2004). “CATA forms alliance with cybersecurity specialist.” *IT Business.ca.* http://www.itbusiness.ca/index.asp?theaction=61&sid=54757 (10 February 2004).

Taft, Darryl K. (2004). “Building Java, .Net Apps Sans Coding.” *EWeek-Enterprise News and Reviews*. http://www.eweek.com/article2/0,4149,1536587,00&.asp (23 February 2004).

Takach, George. *Computer Law*, 2d ed. Toronto: Irwin Law, 2003.

Tan, John. (2001). Atstake Corporate White Paper. “Forensic Readiness.” pp. 1–23. http://www.atstake.com (30 December 2003).

TechRepublic. (2002). “A glossary of security and cyberwarfare terms.” *Tech Republic*. http://www.techrepublic.com (28 December 2003).

TechWeb News. (2004). “ISPs, Telecoms, Others Launch Global Anti-Spam Effort.” *Internet Week*. http://www.internetweek.com/shared/printableArticle.jhtml?articleID=17300952 (15 January 2004).

TechWeb News. (2004). “Security Firm Says Several More Microsoft Vulnerabilities Await Fixes.” http://www.internetweek.com/story/showArticle.jhtml?articleID=17603264 (12 February 2004).

The College of Physicians and Surgeons. (2004). “Fact Sheet – Self Regulation.” http://www.cpso.on.ca/Info_Public/factself.htm (4 February 2004).

The College of Physicians and Surgeons. (2004). “General College Information.” http://www.cpso.on.ca/About_the_College/geninfo.htm (4 February 2004).

The Economist (U.S.) Staff. “A lemon law for software?” *The Economist* (*U.S.*) (16 March 2002).

The Economist (U.S.) Staff. “Coping with the ups and downs.” *The Economist* (*U.S.*) Vol. 339, No. 7963 (27 April 1996): pp. 3–6.

The Economist (U.S.) Staff. (2003). “Fighting the worms of mass destruction.” *The Economist (U.S.)* (27 November 2003). http://www.sfu.ca/~anthonyc/cmpt301/pdf/security.pdf (9 February 2004).

The Economist (U.S.) Staff. (1997). “Hands off the Internet.” *The Economist* (*U.S.*) Vol.343, No. 8024 (5 July 1997): p. 7.

The Economist (U.S.) Staff. “Safe banking.” *The Economist* (*U.S.)* Vol. 339, No. 7963 (27 April 1996): pp. 27–30.

The Insurance Information Institute. (2003). “Most Companies Have Cyber-Risk Gaps in Their Insurance Coverage, States the I.I.I. – Traditional Insurance Policies Not Adequate For Cyber Exposures.” *Insurance Canada.ca.* http://www.insurance-canada.ca/consinfobusiness/IIICyber308.php?format=print (27 February 2004).

The Internet Society (ISOC). (2003). “News from the Internet Society Developing the Potential of the Internet through Coordination, not Governance.” *The Internet Society at the 'World Summit on the Information Society' (WSIS 2003)* http://www.isoc.org/news/7.shtml (12 February 2004).

The Oxford Encyclopaedic English Dictionary. Oxford (UK): Oxford University Press, Clarendon Press; 1991.

The President’s National Security Telecommunications Advisory Committee. (2003).*Internet Security / Architecture Task Force Report – Defining the Edge of the Internet* http://www.ncs.gov/Image-Files/ISATF_Issue_2_final.pdf (12 February 2004).

The SCO Group. (2004). The SCO Group. http://www.sco.com (04 March 2004).

The United States General Accounting Office. (2003). GAO Report Number GAO-03-119, "High-Risk Series-An Update." http://www.gao.gov/atext/d03119.txt (16 January 2004).

The United States General Accounting Office. (2003). GAO Report Number GAO-03-715T. *Homeland Security: Information Sharing, Responsibilities, Challenges, and Key Management Issues - Testimony Before the Committee on Government Reform, House of Representatives* http://www.gao.gov/new.items/d03715t.pdf (20 January 2004).

The United States General Accounting Office. (1996). GAO Report Number GAO/AIMD-96-84. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*. http://www.fas.org/irp/gao/aim96084.htm (3 February 2004).

The U.S. Computer Emergency Readiness Team. (2003). "Best Practices and Standards: Corporate Governance." http://www.us-cert.gov/workwithus/index4.html (31 December 2003).

The White House. (1997). *A Framework for Global Electronic Commerce*. http://www.technology.gov/digeconomy/framewrk.htm (10 December 2003).

The White House. (2003). *The National Strategy to Secure Cyberspace*. http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf (30 December 2003).

Thibodeau, Patrick. "Government Seeks Vendor Accountability; Security directive means agencies will hold vendors responsible for troubled software. *Computerworld* (25 October 1999): p. 14.

Thibodeau, Patrick. "Homeland security bill limits vendor liability: private-sector software may also be affected by bill". *Computerworld* Vol. 36, No. 48 (25 November 2002): pp. 48–54.

Thompson, Clive. (2004). "The Virus Underground." *New York Times Online.* http://www.nytimes.com/2004/02/08/magazine/08WORMS.html?pagewanted=print&position (10 February 2004).

Thurston, Clive. "Bill 124 and the road ahead." *Daily Commercial News* Vol. 76, No. 171 (10 September 2003): p. 5.

Todd, Ewen. 1990. Epidemiology of foodborne illness: North America. The Lancet. Vol. 336, No. 8718: 788–790.

Torrie, Ralph D. (2003). "Electricity Productivity, "DSM" and Sustainable Futures for Ontario." *Presentation on behalf of CANET/CEG to the Ontario Energy Board* Advisory Group on DSM Toronto, October 2003 http://www.oeb.gov.on.ca/documents/directive_dsm_ClimateActionNetwork291003.pdf (16 February 2004).

Trope, Roland L. "In Pursuit of the Feasible: A Limited Warranty Of *Cyberworthiness*." *IEEE Security & Privacy*. [forthcoming in March 2003 issue].

Tutorials Agenda. (2003). http://www.cse-cst.gc.ca/en/symposium/tutorials/monday.html (30 December 2003).

U.S. Department of Homeland Security. (2003). "Ridge Creates New Division to Combat Cyber Threats." http://www.dhs.gov/dhspublic/display?content=915 (30 December 2003).

Vaas Lisa. (2004). "PeopleSoft, You Will Be Assimilated." *EWeek-Enterprise News and Reviews.* http://www.eweek.com/article2/0,4149,1517233,00.asp (5 February 2004).

Vamosi, Robert. (2004). "Security breach on Capitol Hill: Its criminal." http://reviews-zdnet.com.com/AnchorDesk/4520-7297_16-5118530.html?tag=adss (26 January 2004).

Vamosi, Robert. (2003). "We need a new national cybersecurity plan—now." http://reviews-zdnet.com.com/AnchorDesk/4630-7297_16-5111287.html?tag=print (10 December 2003).

Van Kirk, Doug. "What to do when your vendor pulls the plug; IS managers seek legal recourse against software publishers that fail to deliver." *InfoWorld* Vol. 16, No. 5 (31 January 1994): pp. 61–66.

Varian, Hal R. (2000)."Managing On-Line Security Risks." Economic Science Column. *The New York Times.* http://www.nytimes.com/library/financial/columns/060100econscene.html (03 March 2004).

Vaughn-Nichols, Steven J. (2004). "Intel Enters the SCO/Linux Wars on OSDL's Side." *EWeek-Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=116213,00.asp (13 January 2004).

Vaughn-Nichols, Steven J. (2004). "Novell Completes SUSE Acquisition, Details Indemnification Program." *EWeek-Enterprise News and Reviews*. http://www.eweek.com/article2/0,4149,1435577,00.asp (15 January 2004).

Vietor, Richard H.K. 1990. Contrived competition: airline regulation and deregulation, 1925–1988. Business History Review. Vol. 64, No. 1: 61–109.

Vijayan, Jaikumar. (2004). "DDoS attacks: prevention is better than cure." *Computer Weekly*. http://www.computerweekly.com/Article128198.htm (9 February 2004).

Vowler, Julia. “Clearing the legal mist.” *Computer Weekly* (10 June 1993): pp. 24–25.

Vowler, Julia. “Demanding a law for supply.” *Computer Weekly* (5 March 1992): pp. 34–35.

Wagner’s Weblog. (2004). “Security 2004: Fasten Your Seat Belts, Its Going to be a Bumpy Flight.” http://wagblog.internetweek.com/archives/000880.html (28 January 2004).

Warner, Bernhard. (2004). “SCO Debuts New Site as MyDoom Aims at Microsoft.” http://www.reuters.com/newsArticle.jhtml?type=technologyNews&storyID=4262986 (3 February 2004).

Washington Post Staff. (2004). “Congress and Cybersecurity - Government's Pressing Cybersecurity Issues” *The Washington Post* http://www.washingtonpost.com/wp-dyn/articles/A26684-2004Feb9.html (12 February 2004).

Watson, Albert. “Is Bill 124 really necessary?” *Building* Vol. 53, No.2 (April/May 2003): pp. 6–8.

Weiler, Robert K. (2002). “Decision Support: You Can't Outsource Liability For Security.” *Information Week*. http://www.informationweek.com/story/IWK20020822S0003 (24 February 2004).

Wende, David. “Financial Facts and Money Matters: Protecting the auditor from unlimited liability.” *Beyond Numbers* (1 October 2002): pp. 20-21.

Werbach, Kevin D. “Supercommons: Toward a Unified Theory of Wireless Communication,” *Texas Law Review*. [forthcoming in March 2004]. *Social Science Research Network Electronic Library*. http://papers.ssrn.com/sol3/delivery.cfm/delivery.cfm/SSRN_ID456020_code031013670.pdf?abstractid=456020 (3 March 2004).

West Wing Connections. (2003). “Homeland Security Actions.” http://www.whitehouse.gov/homeland/. (30 December 2003).

West Wing Connections. (2003). “National Security.” http://www.whitehouse.gov/response/index.html (30 December 2003).

Wikipedia.org. (2004). “Software Crisis.” *Wikipedia, the free encyclopedia* http://en.wikipedia.org/wiki/Software_crisis (03 March 2004).

Williams, Michael R. (1994). UTEC and Ferut: The University of Toronto’s Computation Centre. IEEE Annals of the History of Computing. Vol. 16, No. 2.

Williams, Patricia. “Bill 124 poses a thorny issue for contractors: proposal would add more to Project costs.” *Daily Commercial News* Vol. 76, No. 37 (21 February 2003): pp. 8–10.

Winn, Jane. (2002). "Legal Framework Needed for Vulnerability Disclosure Liability." *Secure Business Quarterly*. Vol. 2 Issue 3. http://www.sbq.com (30 December 2003).

Wired News Staff. (2004). "Warning: Microsoft 'Monoculture'." http://www.wired.com/news/privacy/0,1848,62307,00.html (17 February 2004).

Wong, Craig. "Power outage across Ontario and northeastern U.S. shows interdependence." *Canadian Press News Wire* (14 August 2003).

World Summit on the Information Society. (2003). "Draft Declaration of Principles." http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!MSW-E.doc (8 January 2004).

Yager, Tom. "Open source takes hold – Tech executives are turning to open source to run mission-critical applications. Does this spell doom for Big Software?" *InfoWorld* Vol. 23, No. 35 (27 August 2001): pp. 49–51.

Yahalom, Raphael. (2002). "Liability Transfers in Network Exchanges." In *Workshop on Economics and Information Security*, University of California, Berkeley May 2002. http://www.sims.berkeley.edu/resources/affiliates/ workshops/econsecurity/econws/46.ps (3 February 2004).

Young, R. Alan. (2002). "Bank Act Reform 2001 and the Banks." *Canadian Banker Magazine.* (January 2002). http://www.cba.ca/en/magazine/getArticle.asp?at_id=201&pm=true (11 February 2004).

Yurcik, William. (2001). "National Missile Defense: The Trustworthy Software Argument." http://www.cpsr.org/publications/newsletters/issues/2001/Spring/yurcik.html (3 February 2004).

ZDNet Reader, Tech Update. (2003)."Can software engineers be held accountable?" http://techupdate.zdnet.com/techupdate/stories/main/Can_software_engineers_be_held_accountable.html (12 December 2003).

Zhang, Xuemei. 1998. A software cost model with warranty cost, error removal times and risk costs. IIE Transactions. Vol. 30, No. 12: 1135–1142.

Ziff Davis Channel Zone. (2003). "Gates: Blazing the Longhorn Trail." *EWeek-Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=113069,00.asp (9 February 2004).