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

# Énoncé de position du gouvernement du Canada relativement à une stratégie nationale pour la protection des infrastructures essentielles

**novembre 2004**

Canada

# Table des matières

# 1. Objet

Dans le présent document, on expose la position du gouvernement du Canada à l'égard de l'élaboration d'une vaste approche nationale en matière de protection des infrastructures essentielles (PIE). Les auteurs veulent ainsi susciter une rétroaction de la part des groupes d'intervenants et jeter les bases d'une stratégie nationale de protection des infrastructures essentielles.

# 2. Renseignements de base

La vice-première ministre, Anne McLellan, a publié la première Politique de sécurité nationale (PSN) du Canada en avril 2004. Dans le cadre de cette politique, on a annoncé deux initiatives interreliées qui mettent l'accent sur la PIE. Premièrement, pour aider les gouvernements fédéral, provinciaux et territoriaux ainsi que l'industrie à relever le défi de la PIE, le gouvernement du Canada publiera un énoncé de position faisant état des éléments clés de la stratégie nationale de PIE proposée. Deuxièmement, comme la sécurité informatique constitue le principal défi transfrontalier auquel font face les infrastructures essentielles du Canada, le gouvernement fédéral renforcera sa capacité de prévoir et de contrer d'éventuelles cyberattaques. On est en train de créer un groupe de travail national de haut niveau, composé de représentants des secteurs public et privé, en vue d'élaborer une stratégie nationale de cybersécurité.

Outre ces deux initiatives, on passe en revue la *Loi sur la protection civile* du gouvernement fédéral afin de tenir compte des nouvelles exigences de la gestion des mesures d'urgence. Ces exigences englobent les aspects suivants : les programmes d'atténuation des risques, la protection des infrastructures essentielles, la cybersécurité, l’échange d'informations entre les ministères fédéraux, les ententes avec les partenaires étrangers et ceux du secteur privé, et la protection de l'information de nature délicate du secteur privé.

Il est essentiel d'élaborer des stratégies de PIE et de sécurité informatique, en plus d'un dispositif législatif moderne et complet, pour assurer le leadership national visant à réduire les vulnérabilités, à détecter les menaces et les risques de façon plus efficace et à améliorer les efforts d'intervention et de reprise des activités, ainsi que le moment où ils sont déployés.

La figure 1 illustre la stratégie recommandée pour le cadre stratégique sous-jacent de l'élaboration réussie d'une stratégie nationale de PIE au Canada.

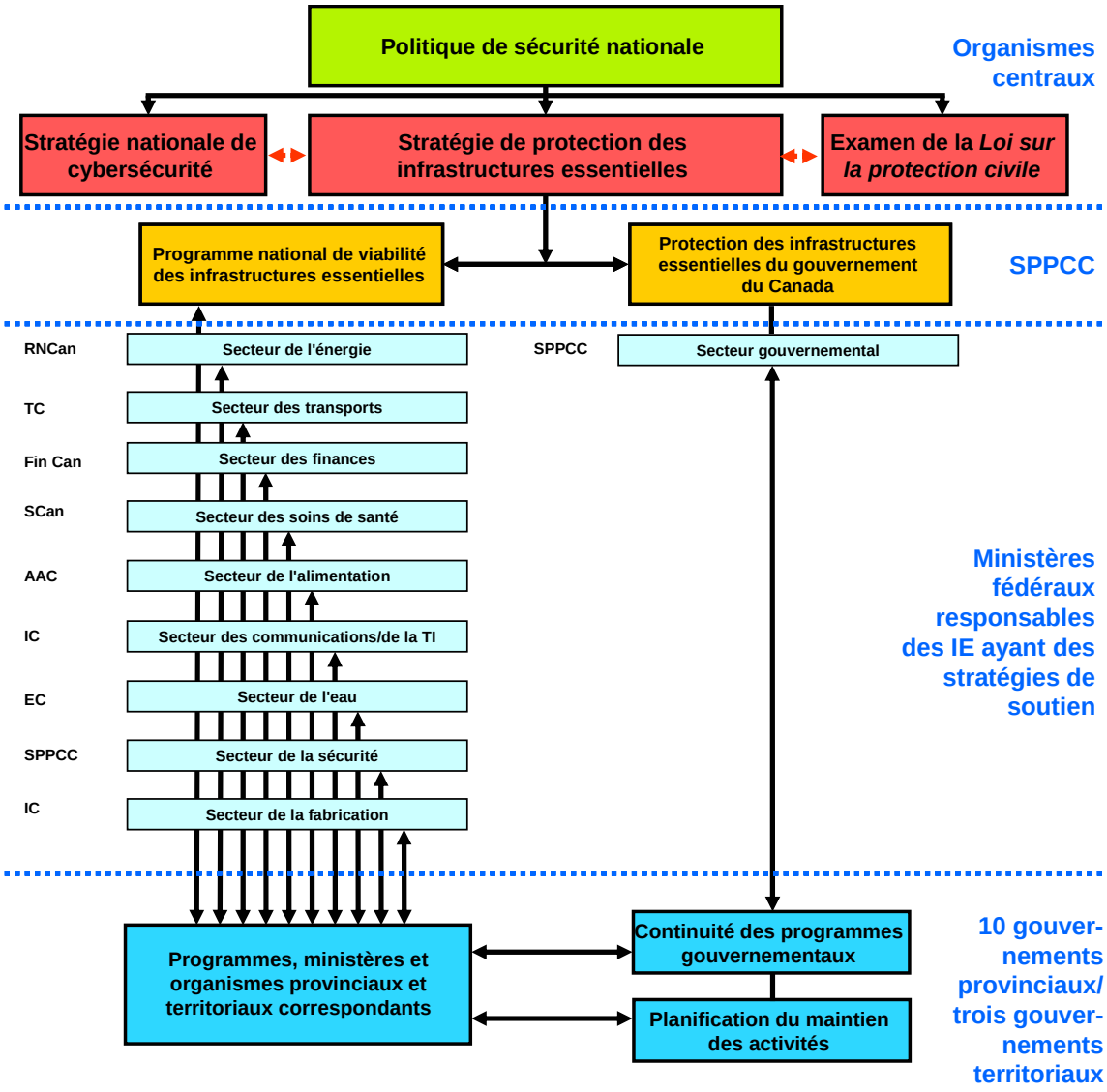


**Figure 1** Approche stratégique recommandée en ce qui a trait à une stratégie nationale de PIE.

## 3. Contexte

Le Canada, les Canadiennes et les Canadiens s'appuient sur des infrastructures essentielles à leur santé, à leur sécurité et à leur mieux-être économique. Ces infrastructures sont très reliées et très interdépendantes. Les fusions d'entreprises, la rationalisation de l'industrie, des pratiques administratives efficientes, comme la fabrication juste à temps, et la concentration de la population dans les centres urbains sont autant de phénomènes qui ont contribué à cette situation. Ce qui est peut-être le plus important, c'est que, au cours des quelque dix dernières années, les infrastructures essentielles du pays sont devenues plus dépendantes de technologies de l'information courantes, notamment Internet. La défaillance ou l'interruption d'un seul système d'infrastructure pourrait s'étendre à d'autres systèmes, causant la défaillance imprévue et de plus en plus grave de services essentiels. De plus, l'interconnexion et l'interdépendance de ces infrastructures les rendent plus vulnérables à une panne ou à la destruction.

Tout comme les vulnérabilités, les menaces changent et prennent de l'importance. Les catastrophes naturelles qui s'abattent sur des infrastructures essentielles sont de plus en plus fréquentes et ont des répercussions de plus en plus grandes. En outre, les infrastructures sont vulnérables dans les environnements où les menaces changent constamment, notamment où il y a des attaques terroristes catastrophiques ou des virus et des vers informatiques destructeurs.

Les Canadiennes et les Canadiens veulent s'assurer que les infrastructures de leur pays sont viables et résistantes. Comme plus de 85 % des infrastructures canadiennes appartiennent au secteur privé et aux provinces et territoires et sont exploitées par ces parties, il faut établir un partenariat national fondé sur un cadre de gestion des risques pour leur fournir cette assurance.

Le Canada définit ses infrastructures essentielles nationales (IEN) comme étant « les installations matérielles et informatiques, les réseaux, les services et les biens matériels dont la perturbation ou la destruction aurait de sérieuses conséquences pour la santé, la sécurité ou le bien-être économique des Canadiens et des Canadiennes ou pour le fonctionnement efficace des gouvernements au Canada. » Les infrastructures essentielles se trouvent dans dix secteurs : énergie et services publics; communication et technologies de l'information; finances; soins de la santé; alimentation; eau; transports; sécurité; gouvernement et fabrication. Ces dix secteurs se divisent en sous-secteurs qui se composent de catégories, afin de refléter et de permettre une analyse plus approfondie de l'infrastructure. Par exemple, le secteur de l'énergie et des services publics se divise comme suit : énergie électrique, systèmes de transmission et de génération du gaz naturel et du pétrole. L'énergie électrique se divise à son tour en divers sous-secteurs : centrales électriques, postes de transmission, corridors de lignes de transport d'électricité (ou lignes de transmission), postes de distribution, centres de contrôle et énergie nucléaire. (Voir l'annexe B pour une liste d'exemples de sous-secteurs).

La façon traditionnelle d'aborder le sujet de la protection des infrastructures nationales est de déterminer les biens particuliers revêtant une importance nationale et d'élaborer des plans pour les protéger. La protection des biens, toutefois, n’est qu'une des nombreuses stratégies dont disposent les propriétaires et les exploitants d'IE pour prévenir les menaces dont peuvent faire l'objet des biens spécifiques et en réduire les vulnérabilités, et ainsi contribuer à rassurer les Canadiens[1]. En raison de la nature diversifiée des infrastructures canadiennes, on doit prendre des mesures de gestion du risque en assurant l'exploitation continue des infrastructures d'un secteur à l'autre, plutôt que dans chaque installation. Par conséquent, le gouvernement du Canada s'efforce d'améliorer la protection là où elle est raisonnable et de trouver des manières de garantir le maintien des services essentiels pour les Canadiens. On peut offrir une protection et une assurance en améliorant la collecte, l'évaluation et la mise en commun d'informations et en assurant la gestion des risques. La protection et l'assurance sont des objectifs permanents que souhaite atteindre le gouvernement du Canada en établissant des partenariats fiables.

L'ex-Bureau de la protection des infrastructures essentielles et de la protection civile (BPIEPC), aujourd'hui Sécurité publique et Protection civile Canada (SPPCC), a publié en novembre 2002 un document de travail pour stimuler le dialogue avec des intervenants sur des concepts et des enjeux qui entourent l'élaboration du Programme national de fiabilité des infrastructures essentielles (PNFIE). Les provinces et les territoires, d'autres ministères fédéraux et des associations de l'industrie ont fait part de

[1] Parmi les autres stratégies possibles, mentionnons la redondance et la sauvegarde, la répartition des opérations, les sources d'approvisionnement multiples, les ententes d'entraide, les avertissements précoces, les interventions rapides, etc.

leurs opinions sur la création du programme et ont présenté de l'information sur leurs programmes et plans existants en matière d'IE. Jusqu'ici, les activités du PNFIE ont visé à réunir les organisations ayant un intérêt envers les IE nationales, dans le but d'établir une stratégie nationale de PIE, des partenariats et des méthodes d'échange d'informations.

On élaborera la stratégie nationale de PIE en se fondant sur les connaissances acquises au cours de l'élaboration du PNFIE et sur les commentaires formulés par les intervenants au cours des consultations. Ces connaissances et cette compréhension communes constitueront le point central de la coordination nationale qui mènera à la création d'une stratégie nationale de PIE. Au sein du gouvernement fédéral, SPPCC et le Secrétariat du Conseil du Trésor (SCT) collaborent à un projet conjoint visant à fixer les priorités et à travailler avec d'autres ministères fédéraux pour protéger les IE du gouvernement du Canada.

## 4. Énoncé de mission

Créer une stratégie nationale intégrée et d'avant-garde pour la protection des infrastructures essentielles avec la participation volontaire des intervenants de l'industrie ainsi que des gouvernements fédéral, provinciaux et territoriaux d'ici l'automne de 2005.

## 5. Résultats escomptés

Le résultat ultime de la stratégie de PIE est de faire en sorte que les IE soient suffisamment résistantes et qu'on puisse donc garantir l'accessibilité continue des services essentiels pour les Canadiens. À moyen terme, la stratégie de PIE visera les résultats suivants :

- Les propriétaires et les exploitants du secteur des IE connaissent et acceptent les responsabilités, les risques et les vulnérabilités de leurs IE et prennent des mesures pour les atténuer;
- Le gouvernement du Canada s'est doté d'un programme permanent pour protéger ses infrastructures physiques et informatiques et montre donc la voie à d'autres secteurs; et
- On met au point et on met en commun de nouvelles connaissances et de nouveaux outils pour la PIE.

# 6. Éléments clés d'une stratégie nationale de protection des infrastructures essentielles

Dans la section suivante, on expose les éléments clés d'une stratégie nationale de PIE. On y trouve entre autres les résultats souhaités de la stratégie nationale ainsi que les processus que l'on doit suivre pour les obtenir.

## 6.1 Principes directeurs

- **Sensibilisation :** La première chose à faire pour prendre des mesures spécifiques consiste à sensibiliser les cadres supérieurs de l'industrie et de tous les ordres de gouvernement à la PIE. Pour ce faire, on doit leur présenter une analyse de rentabilisation qui les convaincra d'effectuer des opérations stratégiques sur le capital (c.-à-d. que l'industrie a une responsabilité fiduciaire d'atténuer les risques pour le bénéfice des parties prenantes, des clients et du grand public au chapitre de la sécurité du public et de la situation économique).

- **Intégration :** On peut assurer la protection des IE en intégrant des questions liées à la sécurité physique et à la sécurité informatique à des programmes de gestion des mesures d'urgence et en favorisant l'intégration de la PIE à de bonnes pratiques d'affaires (comme la planification du maintien des activités) dans les entreprises.

- **Participation :** On ne peut garantir la protection des IE qu'avec la participation de nombreux intervenants de l'industrie et gouvernements fédéraux, provinciaux et territoriaux. Une stratégie nationale doit miser sur les activités et les relations actuelles en ce qui concerne la PIE, celles qui sont établies aussi bien que celles qui sont en train de l'être, et les compléter. Même si la stratégie nationale mettra l'accent sur des initiatives entreprises au Canada, elle doit également reconnaître des activités transfrontalières et internationales.

- **Responsabilisation :** Les partenaires des IE doivent conjointement rendre des comptes aux Canadiens (par l'entremise de la législation, des règlements, des politiques et de la diligence raisonnable) pour sauvegarder leurs propres biens d'IE et garantir la viabilité continue de leurs services.

- **Approche tout risque :** Les IE du Canada pourraient être perturbées ou détruites à la suite d'une attaque délibérée, d'une catastrophe naturelle, d'un accident, d'un virus ou d'une dysfonction informatique. On doit aborder la PIE en tenant compte de tous les risques.

***Selon le gouvernement du Canada, ces cinq principes directeurs influeront sur l'élaboration de la stratégie nationale de PIE.***

## 6.2 Gestion du risque

Les mesures que prennent les partenaires pour assurer la viabilité des IE et les priorités de ces mesures se fondent sur des principes de gestion du risque qui reposent sur des critères communs, le cas échéant[2]. Les partenaires des IE devraient utiliser un ensemble de critères uniforme pour déterminer et classer leurs IE et déterminer le niveau de risque relatif. Pour déterminer le caractère essentiel et prioritaire relatif des biens des IE, on évalue l'*impact* de leur perte sur le fonctionnement du secteur et d'autres secteurs, ainsi que la *conséquence* de leur perte. Les propriétaires et les exploitants prennent des décisions au sujet de la sauvegarde et de l'assurance de la viabilité de leurs propres biens d'IE. Les gouvernements adoptent des méthodes établies pour gérer le risque afin d'assumer leurs responsabilités en ce qui a trait à l'assurance de la fiabilité des IE pour les Canadiens.

Parmi les composantes d'un cadre de gestion du risque pour la PIE, mentionnons les suivantes :

- Compréhension des IE et de leurs interdépendances, et sensibilisation à ces infrastructures;
- Assurance de la fiabilité des IE par l'évaluation, l'atténuation des risques et la préparation en ce qui a trait aux menaces et aux vulnérabilités, et grâce à la recherche-développement;
- Gestion des interventions et de la reprise des activités grâce à une coordination intersectorielle, à la planification des interventions et à l'éducation.

***Selon le gouvernement du Canada, il faut utiliser le cadre de gestion intégré du risque (CGIR) comme point de départ de l'élaboration de la stratégie nationale de PIE.***

## 6.3 Mise en commun de l'information

Comme les IE du Canada sont entre les mains de milliers de différentes organisations – publiques et privées – il faut absolument que les conditions soient réunies pour permettre une mise en commun efficace de l'information. Ces conditions doivent exister non seulement dans les organisations, mais aussi au sein d'un organe de coordination national à l'échelle fédérale.

Les intervenants doivent obtenir de l'information pertinente pour remplir leur rôle relatif à l'assurance de la fiabilité de leurs IE. Plus précisément :

- Les propriétaires et exploitants d'IE devraient posséder de l'information sur les infrastructures essentielles d'autres entités dont ils dépendent, et ils doivent connaître les problèmes qui menacent leurs propres infrastructures pour assurer le maintien des activités;
- Les gestionnaires des mesures d'urgence et les premiers intervenants devraient posséder suffisamment d'informations sur les IE pour planifier et assumer leurs rôles en gestion des mesures d'urgence;

[2] Une approche commune pour déterminer et classer les IE par ordre de priorité est proposée dans l'ouvrage intitulé *Critères de sélection pour déterminer et classer les biens des infrastructures essentielles*, publié en janvier 2004. Voir http://www.ocipep.gc.ca/critical/nciap/nci_criteria_f.asp. Grâce à un cadre de gestion du risque comme celui déposé par le Secrétariat du Conseil du Trésor du Canada, les organisations disposent d'un mécanisme pour élaborer une approche globale face à la gestion du risque stratégique en créant les moyens nécessaires pour analyser, comparer et évaluer des risques essentiellement différents. Voir http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rmf-cgr_f.asp

- Les autorités publiques ayant des responsabilités en matière de protection devraient posséder de l'information sur les infrastructures essentielles de leur administration qui doivent être protégées.

Plus les organisations possèdent d'informations sur les menaces et les vulnérabilités potentielles, plus elles pourront comprendre le risque et assurer la continuité des services essentiels. Parmi les renseignements que l'on doit mettre en commun, mentionnons l'information sur les menaces, les vulnérabilités, les incidents, les mesures de protection et d'atténuation des risques, et les pratiques exemplaires. On peut considérer la mise en commun de l'information comme une façon de mieux gérer le risque et, ainsi, d'aider à décourager, prévenir et atténuer les menaces et d'y réagir.

On reconnaît que la mise en commun de l'information doit se faire dans un climat de confiance et de confidentialité. On devrait recourir le plus possible aux tribunes et mécanismes existants pour échanger de l'information. On étudiera de nouveaux mécanismes de gouvernance, des centres d'intégration de l'information et la modernisation de la législation – en particulier la *Loi sur la protection civile*.

***Selon le gouvernement du Canada, il faut encourager et appuyer l'échange rapide et précis de l'information entre les administrations et les secteurs des IE. Pour ce faire, il faudra mettre sur pied des groupes de travail composés de participants de tous les niveaux et consulter les intervenants, notamment des partenaires à l'échelle internationale, pour déterminer la nature de l'information requise ainsi que le moyen le plus approprié pour échanger de l'information et pour accroître l'interopérabilité.***

## 6.4 Répertoire des biens d'infrastructures essentielles

Il faut cerner les composantes essentielles de chaque secteur pour prendre les mesures nécessaires à la protection et à l'assurance de la fiabilité des IE. En déterminant les composantes des IE et en les classant par ordre de priorité, les gouvernements, les propriétaires et les exploitants peuvent davantage affecter les ressources aux secteurs les plus vulnérables et les plus à risque, élaborer et appliquer des plans, améliorer la capacité d'intervention et appliquer des mesures d'atténuation et de prévention des risques.

Lorsqu'on détermine que des composantes spécifiques de l'infrastructure sont essentielles, on obtient également son lot de problèmes. Par exemple, ce genre d'information peut devenir une cible de choix pour des individus mal intentionnés. Par conséquent, il faut protéger l'information liée aux infrastructures essentielles pour des raisons de sécurité nationale et de sécurité publique, en plus d'intérêts concurrentiels et économiques.

Le gouvernement du Canada utilisera tous ses instruments législatifs et réglementaires pour protéger adéquatement l'information sur les IE.

***Selon le gouvernement du Canada, il doit cibler et évaluer ses propres IE. En outre, le gouvernement du Canada collaborera avec d'autres ordres de gouvernement et le secteur privé pour s'assurer que des processus sont en place pour cibler les infrastructures essentielles (ou leurs composantes) afin de renforcer la sécurité publique et d'adopter de bonnes pratiques de gestion. Le gouvernement du Canada devra s'assurer que tous ces renseignements connexes sont protégés dans toute la mesure que permet la loi.***

## 6.5 Menaces et avertissements

Les intervenants des IE doivent être avertis clairement et rapidement des menaces qui peuvent compromettre les IE pour mettre en œuvre des stratégies de gestion du risque.

Dans la Politique de sécurité nationale, on a souligné que le gouvernement du Canada doit protéger davantage les Canadiens en créant un système de sécurité entièrement intégré qui permettra de réagir plus efficacement aux menaces actuelles et de rapidement s'adapter aux nouvelles. Les partenaires clés – provinces, territoires, collectivités, intervenants de première ligne, secteur privé et Canadiens – seront reliés à ce système.

Le système commence par une évaluation complète des menaces pour le Canada. Cette information est utilisée pour mettre en action des capacités intégrées visant à neutraliser ou à atténuer les incidences de la menace. Lorsqu'un événement survient, un système intégré de gestion des conséquences est mis en action.

Le gouvernement du Canada a mis sur pied un centre d'évaluation intégrée des menaces pour faciliter l'intégration des renseignements recueillis à une évaluation globale des menaces qui sera mise à la disposition de ceux qui en ont besoin. L'approche intégrée adoptée garantit que l'information sera fournie promptement à ceux qui en ont besoin.

Pour fournir aux intervenants des IE des évaluations et des avertissements de menaces plus complets, il faudra recueillir de l'information auprès d'eux, notamment de l'information sur les menaces, les vulnérabilités, les incidents, les mesures de protection et d'atténuation des risques et les pratiques exemplaires.

***Selon le gouvernement du Canada, il faut continuer à améliorer les mécanismes pour communiquer rapidement et efficacement aux intervenants des informations et des renseignements pertinents sur les éléments qui menacent les IE.***

## 6.6 Interdépendances des infrastructures essentielles

Chaque infrastructure est un système complexe et perfectionné en soi, mais les diverses interconnexions et interdépendances entre ces infrastructures et entre elles et la société le sont encore plus. Les interdépendances font en sorte que les infrastructures sont vulnérables aux perturbations ou à des événements qui se produisent dans d'autres secteurs. Elles entraînent un effet domino difficile à prédire qui peut intensifier les impacts de certaines défaillances et les conséquences pour la société. À cette interdépendance vient s'ajouter la dépendance accrue envers les technologies de l'information.

La panne d'électricité d'août 2003 nous a donné une leçon sur les interdépendances des infrastructures, car elle nous a montré comment la défaillance d'une infrastructure peut se répercuter dans d'autres infrastructures. Il s'agit de la plus grande panne à être jamais survenue en Amérique du Nord. Cinquante millions de personnes de New York à Toronto ont été privées d'électricité, certaines pendant deux jours. L'infrastructure de la santé publique de l'Ontario a été mise à rude épreuve parce que les hôpitaux s'alimentaient à même des génératrices d'urgence. On a presque épuisé les sources d'eau et de nourriture. Les épiceries ont été forcées de jeter des milliers de dollars de nourriture, et les usines de traitement des eaux ont dû utiliser des génératrices d'urgence pour poursuivre leurs activités. Des milliers d'Ontariens se sont retrouvés à court d'argent à

cause de la fermeture des banques et de l'interruption du service des guichets automatiques et des banques. Comme les stations-service étaient incapables de pomper l'essence (les pompes fonctionnent à l'électricité), les transports ont été perturbés. Des vols ont été annulés dans les deux aéroports internationaux de l'Ontario (Toronto et Ottawa). Un volume d'appels phénoménal a engorgé les systèmes d'appel d'urgence (911), et les postes de transmission d'ondes cellulaires ont failli à leur tâche après avoir épuisé leurs génératrices de secours.

Par le passé, les initiatives de protection des IE ont été menées par des secteurs ou des industries spécifiques, par des entreprises, des associations sectorielles ou des ministères travaillant en grande partie de façon indépendante. Ces initiatives n'ont pas vraiment réglé les problèmes de liaison entre les infrastructures. Il faut adopter une approche holistique fondée sur des systèmes pour régler pour de bon le problème des interdépendances.

***Selon le gouvernement du Canada, on doit intégrer l'analyse des interdépendances aux décisions relatives à la gestion du risque, aux stratégies d'atténuation et de préparation, ainsi qu'aux interventions et à la reprise des activités. De plus, le gouvernement du Canada coordonnera les efforts nationaux dans la recherche-développement sur les interdépendances, qui sont essentiels à la compréhension de ce problème.***

## 6.7 Gouvernance

Une étude des modèles de gouvernance de la PIE dans d'autres pays révèle l'importance d'établir des partenariats officiels entre les propriétaires et exploitants d'EI et les gouvernements pour assurer l'orientation et la coordination nationales de la PIE[3]. À cette fin, le gouvernement du Canada propose de travailler avec chaque secteur pour élaborer des mécanismes appropriés de gouvernance, le cas échéant. Il reconnaît qu'il peut déjà exister des mécanismes convenables dans certains secteurs, mais qu'il faudra en élaborer d'autres en tenant compte des cadres législatifs et réglementaires existants. Ces mécanismes de gouvernance doivent être inclusifs et reconnaître la dimension régionale des IE, permettant ainsi au gouvernement et au secteur privé de maximiser la coordination et l'intégration des efforts.

Des questions horizontales comme l'analyse des interdépendances, la mise en commun de l'information et la sécurité informatique touchent tous les secteurs. Elles peuvent exiger des mécanismes de gouvernance distincts comme le Groupe de travail sur la sécurité informatique que l'on propose dans la PSN.

La mise en œuvre d'une stratégie nationale de PIE comprend un ensemble d'activités. Il faudra faire appel à une capacité d'envergure nationale pour orienter et intégrer les efforts des structures de régie nationales et internationales avec ceux de l'industrie privée et des gouvernements provinciaux et territoriaux. Les provinces et les territoires, en collaboration avec des ministères fédéraux dans les régions, orienteront les intérêts de l'industrie privée et les intégreront aux administrations des provinces et des territoires, surtout lorsqu'on décrétera l'état d'urgence dans une province ou un territoire.

[3] Pour une analyse des options de gouvernance, voir Edlund and Associates, *Establishment of a National Advisory on Critical Infrastructure Protection*, préparé pour le Bureau de la protection des infrastructures essentielles et de la protection civile, Ottawa (Ontario), 14 juillet 2003, et de Zeta Group, *NCIAP Governance Paper*, préparé pour le Bureau de la protection des infrastructures essentielles et de la protection civile, Ottawa (Ontario), mars 2003.

Le gouvernement du Canada propose de mettre sur pied un organisme national, comme un conseil consultatif national sur la PIE, composé de représentants de tous les ordres de gouvernement et des secteurs de l'industrie. Un tel organisme transformerait des mécanismes de gouvernance sectoriels et les efforts de collaboration du gouvernement et de l'industrie en structures régionales de PIE. L'une des tâches les plus importantes d'un tel organisme consisterait à sensibiliser les représentants de la haute direction de l'industrie et du gouvernement aux questions liées à la PIE et à soutenir la coordination et la gestion horizontales d'initiatives internationales, nationales et régionales de PIE.

***Selon le gouvernement du Canada, il faut établir une architecture de gouvernance qui permettra d'orienter et de coordonner les activités de PIE à l'échelle nationale. À cette fin, il mettra sur pied un organisme national de PIE, soutiendra l'élaboration de mécanismes appropriés dans les secteurs et réglera les problèmes horizontaux et régionaux.***

## 6.8 Recherche et développement

Au moyen d'activités d'extension, de coordination et de promotion, le Canada doit continuer de travailler à mettre en valeur l'expertise et l'innovation considérables de ses chercheurs. Ceux-ci fournissent de nouvelles connaissances et de nouvelles technologies pour la PIE et les efforts liés à la sécurité informatique.

***Selon le gouvernement du Canada, il faut réaliser des projets de recherche ciblés et mettre en valeur les capacités scientifiques et technologiques canadiennes et internationales pour combler les lacunes au chapitre des connaissances, renforcer la capacité nationale et créer des solutions novatrices pour la PIE***

## 6.9 Coopération internationale

Les gouvernements du monde entier se sont mobilisés pour protéger les IE. On peut apprendre de l'expérience d'autres pays et participer à leurs initiatives et activités liées à la PIE. Cela est particulièrement vrai pour les États-Unis, avec qui le Canada partage une infrastructure transfrontalière essentielle.

***Selon le gouvernement du Canada, il faut participer à des initiatives internationales en matière de PIE et renforcer les mécanismes de mise en commun de l'information et les liens opérationnels avec d'autres pays et organisations internationales.***

# 7. Prochaines étapes

Dans l’ensemble, la stratégie nationale de protection des infrastructures essentielles du Canada :

- Reconnaîtra les mesures importantes qu'on prend actuellement ou qu'on a déjà prises pour assurer la fiabilité des IE;
- Présentera et établira des priorités et des échéanciers en ce qui a trait aux initiatives qu'entreprendront les gouvernements et le secteur privé, que ce soit individuellement ou en partenariat;
- Énoncera les principes et les objectifs d'initiatives de protection et de fiabilité;
- Orientera les partenaires des IE et proposera des rôles et responsabilités ainsi que des mécanismes de gouvernance pour favoriser un climat de confiance et établir le partenariat.

La prochaine étape, pour le gouvernement du Canada, consistera à consulter la haute direction des gouvernements provinciaux et territoriaux, des représentants de l'industrie et des partenaires clés d'autres pays au sujet de l'élaboration et de la mise en œuvre d’une stratégie nationale intégrée et d’avant-garde pour la protection des infrastructures essentielles avec la participation volontaire des intervenants de l’industrie ainsi que des gouvernements fédéral, provinciaux et territoriaux d’ici l’automne de 2005.

# Annexe A :
# Résumé des positions du gouvernement du Canada

1. **Principes directeurs :** cinq principes (sensibilisation, intégration, participation, responsabilisation, et approche tout risque) directeurs influeront sur l'élaboration de la stratégie nationale de PIE.

2. **Gestion du risque :** il faut utiliser le cadre de gestion intégré du risque (CGIR) comme point de départ de l'élaboration de la stratégie nationale de PIE.

3. **Mise en commun de l'information :** il faut encourager et appuyer l'échange rapide et précis de l'information entre les administrations et les secteurs des IE. Pour ce faire, il faudra mettre sur pied des groupes de travail composés de participants de tous les niveaux et consulter les intervenants, notamment des partenaires à l'échelle internationale, pour déterminer la nature de l'information requise ainsi que le moyen le plus approprié pour échanger de l'information et pour accroître l'interopérabilité.

4. **Répertoire des biens d'infrastructures essentielles** : il doit cibler et évaluer ses propres IE. En outre, le gouvernement du Canada collaborera avec d'autres ordres de gouvernement et le secteur privé pour s'assurer que des processus sont en place pour cibler les infrastructures essentielles (ou leurs composantes) afin de renforcer la sécurité publique et d'adopter de bonnes pratiques de gestion. Le gouvernement du Canada devra s'assurer que tous ces renseignements connexes sont protégés dans toute la mesure que permet la loi.

5. **Menaces et avertissements :** il faut continuer à améliorer les mécanismes pour communiquer rapidement et efficacement aux intervenants des informations et des renseignements pertinents sur les éléments qui menacent les IE.

6. **Interdépendances des infrastructures essentielles :** on doit intégrer l'analyse des interdépendances aux décisions relatives à la gestion du risque, aux stratégies d'atténuation et de préparation, ainsi qu'aux interventions et à la reprise des activités. De plus, le gouvernement du Canada coordonnera les efforts nationaux dans la recherche-développement sur les interdépendances, qui sont essentiels à la compréhension de ce problème.

7. **Gouvernance :** il faut établir une architecture de gouvernance qui permettra d'orienter et de coordonner les activités de PIE à l'échelle nationale. À cette fin, il mettra sur pied un organisme national de PIE, soutiendra l'élaboration de mécanismes appropriés dans les secteurs et réglera les problèmes horizontaux et régionaux.

8. **Recherche et développement :** il faut réaliser des projets de recherche ciblés et mettre en valeur les capacités scientifiques et technologiques canadiennes et internationales pour combler les lacunes au chapitre des connaissances, renforcer la capacité nationale et créer des solutions novatrices pour la PIE.

9. **Coopération internationale :** il faut participer à des initiatives internationales en matière de PIE et renforcer les mécanismes de mise en commun de l'information et les liens opérationnels avec d'autres pays et organisations internationales.

# Annexe B :
# Secteurs des infrastructures essentielles nationales

SPPCC a déterminé dix secteurs qui constitueront le fondement du PNFIE. Dans le tableau ci-dessous, on énumère ces secteurs ainsi que des exemples de sous-secteurs pour chacun.

| Secteur | | Exemples de sous-secteurs |
|---|---|---|
| 1. | Énergie et services publics | Énergie électrique (production, transmission, énergie nucléaire)<br>Gaz naturel<br>Systèmes de production et de transport du pétrole |
| 2. | Communications et technologie de l'information | Télécommunications (téléphone, télécopieur, câble, satellites)<br>Réseaux de télécommunication<br>Logiciels<br>Matériel<br>Réseaux (Internet) |
| 3. | Finances | Services bancaires<br>Valeurs<br>Systèmes de paiement |
| 4. | Soins de la santé | Hôpitaux<br>Établissements de santé<br>Établissements de distribution de produits sanguins<br>Laboratoires<br>Produits pharmaceutiques |
| 5. | Alimentation | Salubrité des aliments<br>Industrie agroalimentaire<br>Distribution des aliments |
| 6. | Eau | Eau potable<br>Gestion des eaux usées |
| 7. | Transport | Avion<br>Train<br>Bateaux<br>Véhicules routiers |
| 8. | Sécurité | Sûreté chimique, biologique, radiologique et nucléaire<br>Matières dangereuses<br>Recherche et sauvetage<br>Services d'urgence (services de police, d'incendie, d'ambulance et autres)<br>Barrages[4] |
| 9. | Gouvernement | Installations gouvernementales<br>Services gouvernementaux (p. ex. services météorologiques)<br>Réseaux d'information gouvernementaux<br>Biens du gouvernement<br>Symboles nationaux clés (institutions culturelles et sites et monuments nationaux) |
| 10. | Fabrication | Industrie chimique<br>Base industrielle de défense |

[4] Les barrages peuvent être essentiels pour un certain nombre de secteurs (eau, transports, et énergie et services publics) selon leur fonction. Même si différents secteurs doivent assurer la continuité des services offerts par les barrages, leur sécurité est importante pour tous les secteurs. Comme les services que fournissent les barrages et leur sécurité sont interdépendants, on devrait intégrer ces services aux secteurs appropriés. Cependant, on doit s'occuper de la sécurité des barrages dans le secteur de la sécurité.

# Annexe C : Rôles des intervenants

Les gouvernements fédéral et provinciaux/territoriaux du Canada et l'industrie canadienne sont des partenaires des IE. Dans le tableau suivant, on énumère les rôles de ces partenaires et des Canadiens.

| Intervenant | Rôles |
|---|---|
| **Tous les partenaires** | • Élaborer, diriger et gérer des stratégies et des programmes de gestion du risque<br>• Élaborer et diriger des programmes de sensibilisation, de formation et d'éducation<br>• Établir des partenariats entre diverses administrations et mettre l'information en commun<br>• Collaborer à des exercices et à des efforts de R-D<br>• Élaborer et mettre en commun des pratiques exemplaires et des leçons apprises |
| **Gouvernements fédéral et provinciaux/territoriaux** | • Assurer un leadership et une orientation (p. ex. analyser les interdépendances, élaborer des outils, évaluer les progrès et en rendre compte, et régler les problèmes)<br>• Établir des programmes d'assurance de la fiabilité/de protection des IE pour les services gouvernementaux offerts dans leur administration<br>• Participer, avec des propriétaires/exploitants de l'industrie, à des programmes d'assurance de la fiabilité des IE dans les secteurs (notamment lorsque le gouvernement est également un propriétaire/exploitant)<br>• Partager de l'information sur les menaces, les vulnérabilités et d'autres enjeux pertinents en ce qui concerne les sujets pour lesquels le gouvernement possède des renseignements ou un accès exclusif, sous réserve des lois et politiques applicables<br>• Émettre des lignes directrices et des orientations dans des secteurs réglementés par le gouvernement<br>• Élaborer et mettre en œuvre des règlements et des normes<br>• Élaborer des initiatives d'avertissement du public |

| Intervenant | Rôles |
|---|---|
| **Propriétaires/exploitants**[5] | • Renforcer les partenariats réunissant des propriétaires/exploitants et avec des gouvernements<br>• Participer à des programmes de gestion du risque et d'assurance de la fiabilité/de protection des IE dans des secteurs ou sous-secteurs<br>• Mettre en commun l'information sur les menaces et les vulnérabilités en ce qui concerne des sujets où le propriétaire/l'exploitant possède des renseignements ou un accès exclusif |
| **Citoyens** | • S'informer des enjeux relatifs aux IE<br>• Prendre des mesures simples pour protéger des infrastructures comme la TI (c.-à-d. opérations informatiques sécurisées)<br>• Prendre des précautions pour pallier une interruption temporaire de produits et services essentiels |

### *Responsabilités du gouvernement du Canada*

Le gouvernement du Canada a un rôle unique à jouer pour sensibiliser la population, et assurer un leadership national et une collaboration internationale (p. ex. avec le département de la Sécurité intérieure des États-Unis, l'OTAN et le G8). De plus, le gouvernement du Canada protégera ses propres IE, soutiendra des programmes provinciaux/territoriaux et fournira à l'échelle nationale des renseignements uniformes et regroupés sur les menaces et les vulnérabilités. Les principaux ministères et organismes du secteur du gouvernement fédéral représentent le gouvernement canadien dans des initiatives sectorielles d'assurance de la fiabilité/de protection des IE et jouent d'autres rôles dans l'assurance de la fiabilité des IE, notamment :

- Ils favorisent la collaboration entre les partenaires;
- Ils soutiennent des initiatives d'assurance de la fiabilité des IEN et y contribuent;
- Ils permettent la mise en commun de l'information avec des secteurs interdépendants et tous les ordres de gouvernement.

[5] Y compris les administrations fédérales, provinciales et municipales, dans leur rôle de propriétaires/d'exploitants.

Voici la liste des principaux ministères et organismes des secteurs au sein du gouvernement du Canada.

| Secteur | | Ministère/organisme |
|---|---|---|
| 1. | Énergie et services publics | **Ressources naturelles Canada (RNCan)**<br>Soutenu par : Commission canadienne de sûreté nucléaire (CCSN), Commission mixte internationale (CMI), Office national de l'énergie (ONE) |
| 2. | Communications et technologie de l'information | **Industrie Canada (IC)**<br>Soutenu par : Sécurité publique et Protection civile (SPPCC) |
| 3. | Finances | **Finances Canada** |
| 4. | Soins de la santé | **Santé Canada (SCan)** |
| 5. | Alimentation | **Agriculture et Agroalimentaire Canada (AAC)**<br>Soutenu par : Agence canadienne d'inspection des aliments (ACIA), Agence des services frontaliers du Canada (ASFC), Santé Canada |
| 6. | Eau | **Environnement Canada (EC)**<br>Soutenu par : Santé Canada |
| 7. | Transports | **Transports Canada (TC)**<br>Soutenu par : ASFC |
| 8. | Sécurité | **Sécurité publique et Protection civile (SPPCC)**<br>Soutenu par : Santé Canada/Défense nationale (MDN) |
| 9. | Gouvernement | **Sécurité publique et Protection civile (SPPCC) et Secrétariat du Conseil du Trésor (SCT)**[6] |
| 10. | Fabrication | **Industrie Canada**<br>Soutenu par : Défense nationale, Ressources naturelles Canada, Environnement Canada |

[6] SPPCC et le Secrétariat du Conseil du Trésor collaborent à un projet conjoint visant à cerner les ministères fédéraux capables de protéger les IE du gouvernement du Canada, de façon centrale et régionale, à dresser une liste des ministères prioritaires et à travailler avec eux.

Voici la liste des responsabilités fonctionnelles du gouvernement fédéral en ce qui a trait à la PIE.

| **Responsabilités fonctionnelles** | | **Ministères/organismes** |
|---|---|---|
| 1. | Leadership du PNFIE | SPPCC constituera le point central de l'intégration des activités de PIE, de la coordination stratégique et de l'élaboration et de l'intégration de politiques nationales. |
| 2. | Mise en commun de l'information (information sur les menaces et les vulnérabilités/Centre d'évaluation intégrée des menaces – Renseignements sur la sécurité/systèmes d'alerte et d'avertissement) | SPPCC sera le point central de la coordination, de l'analyse et de la mise en commun de l'information sur les menaces et les vulnérabilités (informatique et physique).<br>Autres ministères : AAC, ASFC, ACIA, SCRS, CST, MAECI, MDN, EC, Finances, SCan, RNCan, BCP, GRC, TC (autres ministères/organismes à déterminer) |
| 3. | Sécurité informatique (réseaux et services fondés sur les technologies de l'information) | CST, SCRS, IC, SPPCC, GRC |
| 4. | Gestion des incidents informatiques | SCRS — Incidents liés à la sécurité nationale<br>GRC — Incidents criminels<br>SPPCC, CST — Autres |
| 5. | Sécurité physique | MDN — Militaire<br>GRC — Civil<br>(autres ministères/organismes à déterminer) |
| 6. | Gouvernement du Canada : PIE et stratégies de sécurité informatique | CST, SCRS, SPPCC, TPSGC, GRC, SCT |
| 7. | Recherche et développement | CST, RDDC, IC, CNRC, SPPCC, GRC<br>(autres ministères/organismes à déterminer) |
| 8. | Coordination de la sécurité informatique et de la PIE avec les États-Unis et d'autres pays | ASFC, CST, MAECI, MDN, BCP, SPPC, GRC |

### *Responsabilités de SPPCC*

SPPCC est le ministère fédéral responsable de la PIE. À ce titre, il collaborera avec le SCT à un projet conjoint visant à déterminer les ministères fédéraux capables de protéger les IE du gouvernement du Canada, de façon centrale et régionale, à les classer par ordre de priorité et à travailler avec eux. De plus, SPPCC effectue des analyses de certaines IE et assure la liaison entre les responsables de la sécurité et du renseignement et ses partenaires de la gestion des mesures d'urgence et des IE.

Voici une liste des responsabilités de SPPCC à l'échelle de l'administration centrale et des bureaux régionaux.

| SPPCC | Rôles |
|---|---|
| **Administration centrale** | • Élaboration de la stratégie nationale de PIE<br>• Élaboration du PNFIE<br>• Coordination du PNFIE (ministères/organismes fédéraux responsables, provinces/territoires, associations sectorielles et partenariats avec d'autres pays)<br>• Mise en œuvre du PNFIE (c.-à-d. formation et éducation, information sur les menaces et les vulnérabilités, recherche et développement, etc.)<br>• Assurer la continuité du PNFIE après sa mise en œuvre<br>• Analyse et gestion des risques stratégiques |
| **Bureaux régionaux** | • Soutien et coordination pour les provinces/territoires<br>• Coordination des ministères fédéraux dans les régions<br>• Représente le gouvernement du Canada dans les tribunes régionales au Canada et aux États-Unis<br>• Coordonne la PIE du gouvernement du Canada, par l'entremise de conseils fédéraux |

# Bibliographie

*Awareness, Training and Education for Critical Infrastructure Protection,* Bureau de la protection des infrastructures essentielles et de la protection civile, Ottawa (Ontario), juin 2003.

*Cadre de gestion intégrée du risque*, Secrétariat du Conseil du Trésor du Canada, Ottawa (Ontario) mars 2000. http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rmf-cgr_f.asp

*Cadre stratégique de partage de l'information*, Bureau de la protection des infrastructures essentielles et de la protection civile, Ottawa (Ontario) décembre 2002.

*Critères de sélection pour déterminer et classer les biens des infrastructures essentielles,* Sécurité publique et Protection civile Canada, Ottawa (Ontario), janvier 2004. http://www.ocipep.gc.ca/critical/nciap/nci_criteria_f.asp

Edlund & Associates*, Establishment of a National Advisory Council on Critical Infrastructure Protection (CIP)*, préparé pour le Bureau de la protection des infrastructures essentielles et de la protection civile, Ottawa (Ontario), 14 juillet 2003. Étude inédite.

*Une évaluation des secteurs d'infrastructures essentielles nationales du Canada*, préparé pour le Bureau de la protection des infrastructures essentielles et de la protection civile, Ottawa (Ontario) juillet 2003. http://www.ocipep.gc.ca/critical/nciap/nci_sector1_f.asp

*Guide sur la Loi sur l'accès à l'information* (LAI), Bureau de la protection des infrastructures essentielles et de la protection civile, Ottawa (Ontario) décembre 2002.

*National Critical Infrastructure Protection Project (NCIPP) Concept Paper*, Bureau de la protection des infrastructures essentielles et de la protection civile, Ottawa (Ontario), 27 février 2002.

*Options d'une politique sur le partage de l'information,* Bureau de la protection des infrastructures essentielles et de la protection civile, Ottawa (Ontario) février 2003.

*Outil pour aider les propriétaires et les exploitants à identifier les biens d'infrastructures essentielles,* préparé pour le Bureau de la protection des infrastructures essentielles et de la protection civile, Ottawa (Ontario) 19 décembre 2002.

*Politique sur la sécurité*, Secrétariat du Conseil du Trésor du Canada, Ottawa (Ontario) février 2002. http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_f.asp

*Programme national de fiabilité des infrastructures essentielles (PNFIE) Document de travail*, Bureau de la protection des infrastructures essentielles et de la protection civile, Ottawa (Ontario) novembre 2002. http://www.ocipep.gc.ca/critical/nciap/disc_f.asp

*Programme national de fiabilité des infrastructures essentielles (PNFIE) Mises à jour*, Sécurité publique et Protection civile Canada, Ottawa (Ontario) 2003–2004. http://www.ocipep.gc.ca/critical/nciap/update_f.asp

*Programme national de fiabilité des infrastructures essentielles (PNFIE) Sommaire*, Bureau de la protection des infrastructures essentielles et de la protection civile, Ottawa (Ontario), novembre 2002. http://www.ocipep.gc.ca/critical/nciap/synopsis_f.asp

*Protéger une société ouverte : la politique canadienne de sécurité nationale,* Bureau du Conseil privé, Ottawa (Ontario) Canada, avril 2004. http://www.pco-bcp.gc.ca/docs/Publications/NatSecurnat/natsecurnat_f.pdf

*Site Web de SPPCC* : http://www.sppcc.gc.ca/index.asp

The Zeta Group, *NCIAP Governance Paper*, préparé pour le Bureau de la protection des infrastructures essentielles et de la protection civile, Ottawa (Ontario), mars 2003. Étude inédite.