Sécurité publique Canada | Public Safety Canada

Canada

Bâtir un **Canada sécuritaire** et **résilient**

Renouveler l’approche du Canada face à la résilience des infrastructures essentielles

Rapport sur ce que nous avons entendu

Lisez cette publication en ligne à l'adresse suivante :
https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/rnwng-cnd-pprch-crtcl-nfrstrctr-rslnc-2022/index-fr.aspx

Le présent rapport résume les enjeux soulevés lors des consultations du gouvernement du Canada sur le renouvellement de la Stratégie nationale sur les infrastructures essentielles.

Also available in English under the title: Renewing Canada's Approach to Critical Infrastructure Resilience: What We Heard Report

Sécurité publique Canada (Communications)
269, avenue Laurier Ouest
Ottawa (Ontario) K1A 0P8
Canada

communications@ps-sp.gc.ca

Table des matières

Résumé

Depuis l'automne 2021, Sécurité publique Canada (SP) a entamé un dialogue avec des représentants de l'ensemble du milieu des infrastructures essentielles (IE) sur le renouvellement de la *Stratégie nationale sur les infrastructures essentielles* (Stratégie nationale) de 2009. Les points de vue recueillis lors de ces consultations serviront à l'élaboration d'une vision prospective de la résilience des infrastructures essentielles du Canada.

Ce rapport « Ce que nous avons entendu » passe en revue les principaux thèmes qui ont émergé au cours de l'engagement.

Principes fondamentaux des infrastructures essentielles

Nous avons entendu que la définition actuelle des IE énoncée dans la Stratégie nationale décrit de manière adéquate l'essence des IE. Cependant, certains répondants ont suggéré d'inclure des références aux interdépendances et aux chaînes d'approvisionnement. La majorité des répondants conviennent que le classement actuel des dix secteurs couvre toute l'étendue des infrastructures essentielles du Canada. D'autres ont suggéré que l'ajout des secteurs de l'espace et de la défense, entre autres, serait justifié pour répondre aux menaces et pressions en constante évolution.

Enjeux soulevés dans les objectifs de la stratégie nationale actuelle

Établissement de partenariats : Nous avons entendu que les partenariats pourraient être élargis afin d'impliquer les municipalités et les collectivités autochtones dans les forums sur les IE. Un renforcement des partenariats intersectoriels était au cœur des préoccupations des répondants, ces derniers voulaient aussi s'assurer que des mécanismes soient en place pour un dialogue public-privé en continu.

Approche de gestion tous risques : La complexité liée à l'obtention de lignes directrices et d'avis auprès des divers paliers de gouvernement a été évoquée par les participants. Selon eux, la cohérence et la coordination entre les juridictions sont nécessaires, de même que l'élaboration d'une méthode pour désigner les IE vitales. On propose des fonctions clés pour le gouvernement, dont l'établissement de registres de

données qui pourraient être utilisés pour identifier les menaces et appuyer les pratiques de gestion tous risques.

Échange d'information : Tous sont d'accords que le public et les partenaires du milieu des infrastructures essentielles devraient être inclus dans le partage de l'information sur les risques. En outre, les répondants ont exprimé le désir non seulement de recevoir de l'information, mais aussi de renseigner le gouvernement sur les menaces auxquelles ils sont confrontés. Une gamme de soutiens nécessaires à la résilience a été suggérée, notamment la création d'un Centre national sur les infrastructures essentielles qui servirait de point de convergence pour la coordination.

Propositions d'un nouvel objectif pour la Stratégie nationale

Compte tenu du caractère de plus en plus complexe des menaces émergentes et de la nature interdépendante des opérations des IE, les répondants ont souligné que des précisions au sujet des rôles et responsabilités des divers intervenants doivent être apportés et la reddition de comptes doit être officialisée. Nous avons entendu que la mise en place d'obligations légales pour les IE désignées pourrait favoriser la responsabilisation et améliorer la protection des IE. Les participants ont également souligné le rôle du gouvernement dans la prestation de soutien pour les IE (p. ex. directives, mécanismes de financement, protection contre la responsabilité) pour aider à répondre à toute nouvelle exigence éventuelle.

Contexte

La Stratégie nationale sur les infrastructures essentielles[1] (Stratégie nationale) du Canada a été publiée en 2009 et a été approuvée par les ministres fédéral, provinciaux et territoriaux responsables de la gestion des mesures d'urgence. La Stratégie nationale vise principalement à renforcer la résilience des infrastructures essentielles au Canada. Elle établit un cadre de coopération auquel les gouvernements, les propriétaires et les exploitants peuvent travailler ensemble à la prévention, à l'atténuation, à la préparation, à l'intervention et au rétablissement en cas de perturbation, et ainsi protéger les fondements de notre pays et de notre mode de vie.

Dans le cadre de l'engagement pris dans le Plan d'action 2018-2020 sur les infrastructures essentielles du Forum national intersectoriel[2], Sécurité publique Canada a examiné la Stratégie nationale. Cet examen a révélé que la Stratégie nationale était désuète et qu'elle devrait être renouvelée en collaboration avec le secteur privé, les provinces et territoires, les partenaires fédéraux et les autres parties prenantes.

Le renouvellement de la Stratégie nationale est l'occasion de faire la lumière sur ce qui va bien, ce qui doit être amélioré et ce que devrait être notre vision de l'avenir sur la résilience des IE.

Aperçu de la démarche de participation

Pour assurer la représentation des points de vue de l'éventail des intervenants du milieu des infrastructures essentielles, trois approches ont permis de recueillir des commentaires : un sondage ciblé en ligne; des rencontres et présentations; et des soumissions par courriel.

[1] Sécurité publique Canada. Stratégie nationale de 2009 sur les infrastructures essentielles. https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-fr.aspx

[2] Sécurité publique Canada. Plan d'action 2018-2020 sur les infrastructures essentielles du Forum national intersectoriel. https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/archive-pln-crtcl-nfrstrctr-2018-20/index-fr.aspx

Consultation ciblée en ligne : Parlonsinfrastructuresessentielles.ca

Du 21 avril au 1er juin 2022

Plus de 2 800 intervenants du milieu IE, y compris des fonctionnaires fédéraux, provinciaux, territoriaux et municipaux, des propriétaires et exploitants des IE et des universitaires ont été invités à participer et à diffuser le lien vers la consultation en ligne au sein de leurs réseaux. De plus, le lien a été affiché sur le site Web de SP et sur le site Consultation auprès des Canadiens. Des commentaires ont été sollicités sur des enjeux tels que la modernisation de la définition des IE, la priorisation des IE les plus vitales et le soutien de la gestion du risque face aux menaces complexes et changeantes.

La mobilisation en ligne a permis de recueillir 120 réponses au sondage et 9 idées sur le babillard virtuel. D'après les renseignements recueillis lors de l'inscription des 120 répondants, 41 provenaient du secteur public, 76 du secteur privé et 3 n'étaient pas précisés. Les participants étaient des fonctionnaires, des propriétaires-exploitants, des associations industrielles, des universitaires et des représentants d'autres professions. La représentation régionale était diversifiée; la plupart des participants se trouvant en Ontario.

La majorité (79%) des répondants au sondage proviennent de quatre secteurs : la fonction publique, les technologies de l'information et de la communication, l'énergie et services publics et le transport.

Rencontres et présentations aux intervenants des secteurs public et privé

Des commentaires ont également été reçus dans le cadre de présentations et de discussions tenues auprès de plus de 40 forums et groupes d'intervenants, y compris des comités du gouvernement fédéral, des réseaux sectoriels des IE et auprès des propriétaires et exploitants individuels. Ces réunions ont permis aux partenaires du milieu des infrastructures essentielles d'offrir une contribution et une rétroaction immédiate. Elles ont également mis à profit les relations existantes tout en incluant des intervenants qui ne sont pas actuellement représentés dans la stratégie nationale. De

plus, SP a entamé des discussions avec ses partenaires internationaux, incluant le Groupe des cinq et l’Union européenne.

Présentations transmises par courriel

Les membres du milieu des IE ont également été invités à transmettre leurs points de vue et leurs questions à la boîte de réception des consultations sur les IE (ps.cci-cie.sp@ps-sp.gc.ca). Dix présentations ont été reçues par courriel, incluant des contributions collectives de grandes organisations.

Ce que nous avons entendu

Principes fondamentaux des infrastructures essentielles

Définition

> « La définition actuelle pourrait être améliorée en intégrant l'idée que la façon dont les Canadiens perçoivent les infrastructures essentielles reflète les valeurs et les intérêts du Canada et favorise la solidité du tissu social canadien […] L'incarnation des interdépendances renforcerait également cette définition. » [traduction]
>
> - Participant virtuel

La Stratégie nationale sur les infrastructures essentielles de 2009 définit les infrastructures essentielles comme étant des « processus, des systèmes, des installations, des technologies, des réseaux, des biens et des services nécessaires pour assurer la santé, la sûreté, la sécurité ou le bien-être économique des Canadiens et des Canadiennes ainsi que l'efficacité du gouvernement. Il peut s'agir d'infrastructures autonomes ou caractérisées par des interdépendances au sein d'une province ou d'un territoire, entre eux ou au-delà des frontières du pays. La perturbation de ces infrastructures essentielles pourrait se traduire en pertes de vie humaines et en effets économiques néfastes, et pourrait considérablement ébranler la confiance du grand public. »

Interrogés sur la question à savoir si la définition actuelle des infrastructures essentielles saisit bien leur essence, la plupart des répondants (70 %) ont répondu par l'affirmative.

Certains répondants ont recommandé d'ajouter l'aspect des interdépendances des IE à la définition. Ces suggestions concernaient surtout la prise en compte des chaînes d'approvisionnement, des systèmes cybernumériques et de l'environnement naturel. Les répondants qui ont indiqué le besoin d'inclure les systèmes numériques ont souligné l'importance de protéger les données et l'information ainsi que d'envisager la sécurité de l'approvisionnement du matériel et des logiciels. Les enjeux récents et continus liés aux chaînes d'approvisionnement permettant la circulation des biens ont été mentionnés, ainsi que l'importance de tenir compte des sous-traitants et des fournisseurs qui offrent leurs services aux IE.

Enfin, les répondants ont indiqué que la définition pourrait être améliorée en incluant la notion de risque ou d'incidence. À titre d'exemple, on a souligné que les perturbations des IE peuvent avoir d'importantes conséquences sur l'environnement et la population canadienne.

Configuration des secteurs

La Stratégie nationale sur les infrastructures essentielles de 2009 a recensé les dix secteurs suivants :

- Énergie et services publics
- Finances
- Alimentation
- Gouvernement
- Santé
- Technologies de l'information et de la communication
- Secteur manufacturier
- Sécurité
- Transport
- Eau

La définition et la liste connexe des dix secteurs fournissent une compréhension commune des IE à l'échelle nationale et constituent le fondement de l'engagement en matière d'IE avec le gouvernement fédéral. Bien que les dix secteurs ne saisissent pas nécessairement toute la totalité des IE au Canada, la plupart des répondants estimaient qu'ils représentaient adéquatement l'étendue des IE au Canada. Toutefois, il a été mentionné que des précisions étaient nécessaires pour déterminer les biens et les systèmes qui sont inclus dans chacun des secteurs.

Les répondants ont été invités à choisir, parmi plusieurs nouveaux secteurs suggérés, ceux qui pourraient être considérés comme des IE, puis de proposer d'autres secteurs d'IE.

Espace : Le secteur potentiel de l'espace a reçu le plus d'appui pour être reconnu comme un secteur distinct en raison du rôle essentiel que joue l'infrastructure spatiale dans le soutien de toutes les autres formes d'IE et de surveillance environnementale. À l'heure actuelle, l'infrastructure spatiale, comme par exemple les satellites de télécommunication qui relient les Canadiens d'un océan à l'autre, fait partie du secteur

de la Technologies de l’information et de la communication (TIC). Toutefois, les biens, les systèmes et la technologie spatiaux exercent des fonctions au-delà des TIC. Le service spatial le plus connu est sans doute le Système mondial de localisation (GPS), un système mondial de navigation par satellite qui transmet des données sur la position, la synchronisation et la navigation aux Canadiens. Certains répondants ont souligné que plusieurs services essentiels sont fournis par l'infrastructure spatiale, comme par exemple la navigation dans les communautés nordiques au moyen de la cartographie des glaces et la surveillance des cultures pour l'agriculture de précision. On a aussi souligné que les biens spatiaux appuient aussi la recherche scientifique, comme l’étude de la météo spatiale.

> « Le Canada dépend des systèmes spatiaux pour un large éventail d’activités quotidiennes essentielles. L’espace relie les Canadiens d’un océan à l’autre, facilite et favorise les activités commerciales courantes et l’échange de biens, de services et d’information partout dans le monde et soutient la sécurité et la sûreté nationales. » [traduction]
>
> - Participant virtuel

Défense et sécurité : Bien qu’il ne s’agisse pas de l’un des choix de réponse, plusieurs répondants se sont prononcés en faveur de la création d’un secteur distinct de la défense et de la sécurité afin de refléter l’importance de ces derniers pour la sécurité et la prospérité du Canada. Actuellement, la défense et la sécurité constituent un sous-secteur du secteur gouvernemental, et le secteur manufacturier englobe la base industrielle de la défense.

Infrastructure communautaire : Les participants qui perçoivent l’infrastructure communautaire comme un secteur des IE ont fait valoir que l’infrastructure communautaire fournit des services essentiels divers, comme la santé publique, l’éducation (garderies et écoles), le logement et les travaux publics (en particulier les installations publiques et les ressources humaines). Ces services essentiels jouent un rôle important dans la promotion de la résilience individuelle et collective, ce qui améliore la résilience de l’ensemble de la collectivité. Pour les communautés autochtones, cela peut inclure les centres de guérison et les centres d’Aînés. L’inclusion de l’infrastructure prioritaire autochtone en tant que secteur distinct a également été proposée.

Milieu universitaire et de la recherche : Les répondants ont mentionné la double fonction du milieu universitaire et de la recherche. En première partie, les instituts

d’enseignement supérieur et de recherche produisent de la propriété intellectuelle et sont exposés à des menaces internes. En deuxième partie, ces institutions jouent un rôle clé dans la production de technologies émergentes (p. ex. quantique, technologies propres, Internet des objets, biologie synthétique) qui ne correspondent pas toujours parfaitement aux secteurs existants de l’IE et qui doivent être gérées, protégées et sécurisées.

Institutions démocratiques : Les répondants qui ont répondu favorablement ont choisi les institutions démocratiques en partie en notant l'impact des manifestations et d'autres menaces telles que la désinformation et les cyberactivités malveillantes. Il a été mentionné que les institutions démocratiques sont importantes pour maintenir la continuité des services gouvernementaux et éviter les tensions sociales. Enfin, certains répondants se sont interrogés sur l’interaction entre les institutions démocratiques et le secteur gouvernemental existant, en se demandant si les institutions démocratiques constituent un sous-secteur du secteur gouvernemental, ou l’inverse.

Infrastructures naturelles : Les partisans de l'ajout d'un secteur consacré aux infrastructures naturelles ont fait valoir que ce secteur est hautement interdépendant de tous les autres secteurs et qu'il est essentiel à la santé et à la survie de l’homme. De plus, les infrastructures naturelles remplissent de multiples fonctions essentielles, comme la prestation de services municipaux et écosystémiques essentiels qui protègent contre les répercussions des changements climatiques et des phénomènes météorologiques extrêmes.

Objectifs de la Stratégie nationale sur les infrastructures essentielles

> « Il faudrait adopter une approche pangouvernementale à l’égard de la résilience des infrastructures essentielles, car les plateformes d’échange d’information avec les exploitants d’infrastructures essentielles établissent un lien de confiance qui permet d’acquérir une compréhension complète et commune des risques et des vulnérabilités; permettent de coordonner les outils stratégiques nationaux afin d’encourager les secteurs des IE à investir et à atteindre les objectifs de résilience. De cette façon, le gouvernement est en mesure de soutenir et de prioriser les ressources pour protéger et restaurer les IE les plus vitales. L’établissement de

> normes et de règlements pour les IE vitales améliorerait la résilience globale des IE du Canada. » [traduction]
>
> - Participant virtuel

La Stratégie nationale sur les infrastructures essentielles de 2009 était fondée sur les trois objectifs énumérés ci-dessous.

- Établir des partenariats.
- Mettre en œuvre une approche de gestion tous risques.
- Favoriser l'échange en temps opportun de l'information entre les partenaires et la protection de cette information.

Certains répondants ont souligné l'importance de revoir périodiquement les objectifs de la Stratégie nationale, compte tenu du contexte d'exploitation des IE qui est en constante évolution au Canada. En outre, certains ont proposé une surveillance et une évaluation afin de mesurer l'efficacité des mesures prises pour accroître la résilience des IE. Nous avons également demandé aux répondants si les objectifs actuels de la Stratégie nationale sont toujours pertinents. Sur cette question, les réponses étaient partagées; 56 % des répondants ont dit que les objectifs pourraient demeurer inchangés.

La section suivante présente les points de vue et les commentaires des répondants sur les objectifs actuels et la façon dont ceux-ci pourraient être améliorés. Ces commentaires ont ensuite été classés en différentes catégories d'enjeux, pour chaque objectif ainsi que pour la Stratégie nationale dans son ensemble.

Enjeux soulevés pour l'objectif 1 : Partenariats

I. Partenariats élargis

> « Les provinces et les municipalités doivent participer aux IE qui sont exploitées dans leur sphère d'influence. » [traduction]
>
> - Participant virtuel

Les participants ont indiqué que des partenariats pourraient être établis avec de nombreux partenaires non traditionnels, tels que les municipalités. En outre, le gouvernement fédéral pourrait renforcer les réseaux sectoriels existants, agissant à titre de coordonnateur de l'analyse des risques sectoriels et industriels.

Les municipalités ont été identifiées à plusieurs reprises comme manquant de représentation dans la configuration actuelle du secteur de l'IE et dans les structures de mobilisation. Les répondants ont souligné que les perturbations des IE – y compris les répercussions en cascade – peuvent se faire sentir à l'échelle communautaire. Par conséquent, les mesures qui améliorent la résilience des IE améliorent aussi directement la résilience de la collectivité. De nombreux répondants ont fait valoir que les municipalités ont besoin de plus de soutien, car elles n'ont souvent pas les moyens financiers ni la capacité d'effectuer une analyse des interdépendances. Certains répondants étaient d'avis que d'autres partenaires non traditionnels des IE, comme le milieu universitaire et les communautés autochtones, pourraient bénéficier de partenariats pour l'échange d'information, la sensibilisation et pour mettre en œuvre des mesures d'amélioration de la résilience.

II. Collaboration intersectorielle

> « L'efficacité de la gestion du risque dépend de la capacité du milieu des infrastructures essentielles à mobiliser l'ensemble des secteurs pour faciliter une compréhension commune du risque et intégrer une vaste gamme d'activités pour gérer le risque et saisir […] les dépendances connexes qui peuvent avoir des répercussions intersectorielles et intrasectorielles en cascade. » [traduction]
>
> - Participant virtuel

Les répondants ont souligné le besoin de collaboration entre les secteurs des IE et d'avantage d'analyses sur les interdépendances. On souligne que la collaboration intersectorielle aidera à atténuer les vulnérabilités dans des domaines comme les ressources humaines, la technologie de l'information et de la communication, les chaînes d'approvisionnement, l'environnement et les cybersystèmes.

Les récents événements, comme les blocages à Ottawa et aux postes frontaliers entre le Canada et les États-Unis et la pandémie de COVID-19, ont pris le premier plan dans les réponses des intervenants sur les défis liés aux interdépendances des IE. De nombreux répondants ont convenu que le gouvernement du Canada pourrait jouer un rôle important en collaborant avec les secteurs des IE pour les aider à mieux comprendre leurs interdépendances avant qu'un événement survienne.

Il a également été souligné que le gouvernement du Canada devrait continuer de coordonner les partenariats intersectoriels et publics-privés. Certains répondants ont

encouragé le gouvernement du Canada à tirer parti de ses relations existantes avec ses alliés internationaux pour favoriser la collaboration internationale entre les intervenants.

Nous avons entendu que l'identification et la communication des besoins des intervenants du milieu des IE au gouvernement et aux autres parties prenantes sont importants pour établir des partenariats. Les suggestions suivantes ont été formulées :

- Renforcer les partenariats entre les différents échelles de gouvernement et les industries du secteur privé.
- Établir des groupes de travail ou des forums thématiques intersectoriels.
- Mettre sur pied des tribunes fiables pour les principaux exploitants d'IE afin de discuter ouvertement des activités et des besoins en dehors des intérêts commerciaux concurrentiels et exclusifs.
- Établir des rôles et des responsabilités clairs.
- Organiser des réunions intersectorielles pour certaines régions.
- Favoriser la participation à des études sur l'interdépendance dirigées par les parties prenantes.
- Mettre en œuvre des exercices intersectoriels.

Enjeux soulevés pour l'objectif 2 : Approche de gestion tous risques

I. Méthodologie d'évaluation de la criticité nationale

> « Toute méthodologie doit s'adapter aux besoins changeants de la société. La capacité des IE à résister aux perturbations successives ou qui se chevauchent devrait être une des considérations à ajouter. » [traduction]
>
> - Participant virtuel

À l'échelle communautaire, les infrastructures peuvent jouer plusieurs rôles en cas d'urgence. Certaines infrastructures pourraient devenir plus ou moins critiques dans des conditions particulières. Cet état variable peut être décrit comme une criticité dynamique. Pour appuyer la nature dynamique des IE, les intervenants ont proposé diverses approches au cours de la consultation.

Certains répondants ont indiqué que le gouvernement pourrait adopter une approche à plusieurs niveaux pour les secteurs des IE, selon laquelle les secteurs d'IE fortement interdépendants seraient considérés comme des secteurs de niveau 1, comme l'énergie et les technologies de l'information et de la communication, tandis que d'autres secteurs moins essentiels pourraient être des secteurs de niveau 2 ou 3. Parmi les secteurs moins critiques inclus dans ces commentaires, mentionnons les monuments nationaux, les installations commerciales et le milieu universitaire et de la recherche.

La majorité des répondants (84 %) étaient d'avis que des critères devraient être élaborés pour déterminer et prioriser les secteurs, les organisations ou les biens les plus essentiels des IE. Nous avons appris qu'il fallait clarifier l'ordre de priorité du rétablissement des IE en cas d'urgence. Certains moyens ont été suggérés pour élaborer une méthode d'évaluation de la criticité, tels que : l'utilisation de grilles de notation matricielle (mesures de la probabilité et de la gravité), et; par type de collectivité (grande, petite, éloignée, urbaine) au niveau provincial, territorial et fédéral. Un nombre important de répondants ont également suggéré d'utiliser une approche dynamique axée sur le risque en tenant compte des facteurs et des paramètres suivants :

- interruptions qui causent des pertes massives, des maladies, des blessures ou des évacuations;
- population touchée et données démographiques de la collectivité;
- géographie (y compris le risque pour les régions éloignées et isolées, la proximité des dangers naturels);
- dommages économiques potentiels, maturité du marché et dépendance envers des entités étrangères;
- points de défaillance uniques et disponibilité de solutions de rechange;
- portée et nature des interdépendances;
- délais de remplacement des infrastructures endommagées ou vieillissantes;
- incidences juridiques;
- réputation, moral, culture.

Les répondants ont également mentionné la nécessité d'assurer la cohérence de la composition des IE à l'échelle provinciale et territoriale, puisque de nombreux services d'IE sont offerts dans plusieurs administrations du Canada.

II. Gestion du risque fondée sur des données probantes

> « [Il faut] mettre en place des systèmes normalisés de communication et de production de rapports pour l'industrie à l'échelle des divers secteurs afin de cerner les risques et les menaces potentiels et de signaler les incidents. L'industrie et les organismes de sécurité publique pourraient gérer ces systèmes et y avoir accès pour interagir, communiquer (diffuser de l'information) et exploiter l'information et les données. » [traduction]
>
> - Participant virtuel

Les répondants ont souligné la nécessité que la gestion tous risques soit fondée sur des données probantes et que les gouvernements procèdent à une analyse prospective des risques afin d'offrir un soutien proactif pour les IE à l'égard des risques émergents.

On propose d'établir des registres, qui seront tenus par SP, à partir des données des rapports obligatoires sur les IE (p. ex. incidents, plans de continuité des activités, plans d'intervention et de rétablissement des activités, propriété et cyberpratiques) et des rapports volontaires par d'autres IE. Ces registres pourraient être analysés pour identifier les menaces, communiquer de l'information en temps opportun et guider les propriétaires et les exploitants d'IE.

Les répondants ont indiqué qu'un environnement de plus en plus complexe des menaces émergentes, combiné à la nature de plus en plus interdépendante des IE, justifie un soutien accru de la part du gouvernement fédéral. La probabilité croissante de risques qui se chevauchent (c.-à-d. plus d'un événement se produisant simultanément) a également été mise en évidence dans les réponses au sondage.

Plus précisément, de nombreux répondants ont exprimé la nécessité d'obtenir de l'aide pour comprendre les risques existants et émergents liés à leurs activités. Certains ont indiqué qu'ils aimeraient que le gouvernement participe à un plus grand nombre d'évaluations et d'analyses tous risques et communique les résultats de ces analyses en temps opportun. Cette analyse des risques pourrait comprendre des renseignements exploitables pour orienter la réponse de l'institution. Les répondants ont indiqué que les risques suivants nécessitent un examen plus approfondi :

- les cyberrisques, y compris les risques liés à l'acquisition de matériel et de logiciels, les cyberactivités malveillantes et les cyberrisques physiques;

- les risques émergents, comme les pandémies, les changements climatiques et les phénomènes météorologiques extrêmes et les manifestations;
- les risques propres aux interdépendances, comme le risque de répercussions en cascade, les risques pour les réseaux des technologies de l'information et de la communication, les chaînes d'approvisionnement, les cybersystèmes et les risques pour l'environnement naturel.

Enjeux soulevés pour l'objectif 3 : Échange d'information

I. Sensibilisation de la collectivité

> « Il devrait aussi y avoir une composante publique […] pour que les Canadiens comprennent l'importance des infrastructures essentielles et leurs interdépendances. » [traduction]
>
> - Participant virtuel

Les participants ont reconnu qu'il est important d'éduquer et de sensibiliser l'ensemble du milieu des IE et le public. Parmi les idées proposées, on retrouve des campagnes communautaires d'éducation sur les risques et des campagnes d'information publique visant à fournir au grand public des conseils et de l'information sur diverses menaces (par exemple, cyberactivité malveillante dans le contexte de conflits internationaux ou de pandémies mondiales).

Une autre suggestion était la création d'un dépôt public d'information qui serait accessible à l'ensemble du milieu des IE et au grand public. L'information communiquée par l'entremise de ce média pourrait comprendre des directives sur les menaces et les vulnérabilités, des renseignements déclassifiés sur les risques (qui pourraient être tirés des rapports sur les risques et les incidents liés aux IE), des pratiques exemplaires élaborées par des entités d'IE importantes et des directives aux collectivités sur la détermination des IE. Il a été proposé que l'échange d'information soit multidirectionnel, plutôt que de servir de service gouvernemental aux intervenants. Les intervenants des IE souhaitent participer à la prise de décisions au moyen de mécanismes d'échange d'information opportuns et exploitables.

II. Outils de soutien

> « Créer, en partenariat avec les responsables des dix secteurs des IE et le secteur privé ([pour] le financement et l'expertise spécialisée), des centres de connaissances

> spécialisés pour les domaines à risque élevé et les nouveaux enjeux. Cela peut se faire en partenariat avec les universités et les organisations de services professionnels du secteur privé afin [de ne pas] limiter la capacité des fournisseurs de services de l'industrie d'être concurrentiels. » [traduction]
>
> - Participant virtuel

Les répondants ont souligné que le soutien du gouvernement est un élément crucial de leur résilience. Les répondants ont fait diverses suggestions de mesures de soutien, notamment le soutien financier, l'échange d'information et la gestion des enjeux.

En ce qui concerne le soutien aux IE fondé sur les risques, les répondants ont mentionné un besoin pour les mesures de soutien suivantes :

- développement des capacités : éducation et formation; exercices.
- documents d'orientation : rôles et responsabilités par secteur; lignes directrices par secteur; documents d'orientation fondés sur des données probantes (p. ex. sur des menaces précises); avis sur les risques émergents.
- évaluations : répercussions, résilience et capacités.
- outils : registre des pratiques exemplaires, outils de modélisation, registre des risques.
- formation ou financement de personnel spécialisé (p. ex. experts en cybersécurité).

III. Coordination

> « [Il y a] un manque de concentration des responsabilités, de l'information et de l'autorité étant donné l'étendue des industries, des compétences et des organismes non officiels. La CISA est un bon exemple de concentration des pouvoirs, de clarté des responsabilités et où l'échange d'information de grande qualité (au sein du gouvernement et auprès du public) se déroule à un rythme beaucoup plus rapide et où l'information est diffusée efficacement en temps réel aux organisations qui en ont besoin… Ce pourrait être un modèle à envisager. »
>
> - Participant virtuel

Les participants ont souligné le besoin d'un leadership conjoint afin d'améliorer la coordination de la gestion des lignes directrices, des enjeux et des incidents. Les répondants ont aussi demandé davantage de clarté et de cohérence au sujet des rôles

et des responsabilités des divers acteurs des IE qui œuvrent dans différentes juridictions.

Plus précisément, certains répondants ont plaidé en faveur d'un organisme centralisé faisant autorité, ou d'un centre national des IE, qui servirait de guichet unique pour le soutien et la coordination des IE. Les répondants ont expliqué qu'un tel centre de coordination des activités des IE pourrait servir :

- une plateforme de soutien des capacités des IE (p. ex. éducation et formation, lignes directrices, exercices, évaluations et leçons retenues);
- à coordonner la gestion des enjeux au moyen d'un échange d'information opportun et exploitable, aux intervenants FPTMI (fédéraux, provinciaux, territoriaux, municipaux et autochtones) et aux secteurs et leurs ministères fédéral responsable;
- à faciliter la collaboration entre les intervenants des IE et les experts en la matière du milieu universitaire et d'autres travailleurs spécialisés;
- à fournir une vision harmonisée du paysage intergouvernemental des incitatifs en matière d'IE;
- à fournir un soutien cohérent aux IE désignées;
- à fournir une expertise avancée en analyse de données;
- à fournir un soutien en matière de gestion des urgences à l'égard des IE (soutien en temps opportun, intervention en cas d'incident, priorisation, formation en gestion des urgences, gestion des interventions et du rétablissement) et à coordonner l'intervention en cas d'urgence à l'échelle des administrations.

Enjeu soulevé parmi les objectifs de 2009 : La protection des infrastructures essentielles

I. Désignation et protection

> « Afin de maintenir un réseau résiliant d'infrastructures vitales et de services essentiels interconnectés – en effet, les IE vitales doivent être désignées pour mettre en place des normes et une gouvernance qui assureront que les plans appropriés de protection, d'intervention et de rétablissement sont en place. » [traduction]
>
> - Participant virtuel

La grande majorité des répondants au sondage (85 %) ont convenu que les IE les plus vitales devraient être désignées et être tenues de respecter certaines obligations règlementaires. Dans ce contexte, la « désignation » signifie l'identification officielle des entités ou des biens d'IE aux fins de protection et de soutien.

Les participants ont noté qu'établir des réglementations aiderait à fournir une standardisation des services dans le système des IE, ce qui améliorerait sa résilience dans son ensemble. Bon nombre de répondants ont mentionné que l'établissement de niveaux de protection de base permettrait à leur organisation d'avoir confiance envers les IE dont ils dépendent en amont, ce qui leur permettrait d'ajuster leurs plans de continuité des activités, d'intervention et de rétablissement. Les répondants ont également souligné le rôle important que le gouvernement pourrait jouer dans l'établissement de normes et de gouvernance rigoureuses afin d'assurer le respect des obligations et la mise en place de plans de protection, d'intervention et de rétablissement appropriés.

Tel qu'illustré dans la discussion portant sur la méthodologie d'évaluation du caractère critique des infrastructures essentielles vitales, les répondants ont proposé un éventail de facteurs pouvant être combinés afin de déterminer les IE vitales, y compris l'importance de l'infrastructure pour la vie et la santé, la sécurité nationale (ou l'impact de sa défaillance sur la sécurité nationale) et la présence de points de défaillance uniques (p. ex. l'unique voie d'accès à une collectivité éloignée).

En outre, plusieurs participants ont dit que les systèmes hautement interdépendants devraient être officiellement désignés et réglementés, compte tenu de leur potentiel à entraîner la défaillance en cascade d'autres IE et d'avoir des répercussions néfastes sur les collectivités et la société canadienne. Ces répondants ont ciblé les secteurs des transports, de l'énergie et des services publics et de la technologie de l'information et de la communication à cette fin. De plus, les répondants ont noté que les cybersystèmes et l'infrastructure spatiale ont le même niveau élevé d'interdépendances avec d'autres secteurs des IE, ce qui pourrait également nécessiter une réglementation pour protéger le système global des IE.

II. Obligations et rapports d’états

> « La responsabilisation comprend la propriété, les pratiques, la protection des renseignements personnels, l’autovérification, la production de rapports et la surveillance. » [traduction]
>
> - Participant virtuel

Nous avons entendu que la création d’un cadre de réglementation national pour les IE augmenterait la résilience globale du système, ce qui améliorerait la sécurité et la confiance. Certains ont soulevé l’importance d’assurer la cohérence des nouveaux règlements auprès des régulateurs sectoriels et des juridictions provinciales et territoriales, afin d’éviter un environnement réglementaire encombrant et un fardeau redditionnel redondant.

Voici quelques obligations suggérées par les répondants :

- Normes obligatoires et normes de service
- Normes internationales (ISO)
- Rapport en cas d’incident
- Cyberpratiques
- Participation à des exercices
- Plans d’intervention et de rétablissement
- Plans de continuité des opérations
- Divulgation de renseignements sur la propriété

Quelques répondants ont également recommandé la déclaration obligatoire des adresses IP et des renseignements sur la géolocalisation dans le but explicite de faciliter les interventions d’urgence en temps opportun.

Advenant que les IE vitales soient désignées, des répondants ont suggéré que le gouvernement se serve des pratiques exemplaires existantes ayant été recueillies auprès IE vitales pour faciliter l’établissement d’un consensus sur l’approche, la responsabilité et l’état final, ce qui permettrait aux IE plus petites et non désignées de satisfaire aux normes visant les IE plus importantes et plus matures.

Bien que de nombreux répondants conviennent que la communication de rapports d’états constitue une partie importante d’un cadre réglementaire, bon nombre d’entre eux soulignent l’importance d’assurer la protection des données transmises. Les participants ont donc recommandé que toute information communiquée au grand public

soit nettoyée de données identificatoires et de renseignements exclusifs d'intérêt commercial, ou que ces données soient agrégées.

III. Mesures incitatives

> « Un soutien financier est nécessaire pour faciliter la transition vers un cadre réglementaire. Le soutien peut être direct ou indirect. Le soutien direct pourrait comprendre de l'aide pour la dotation, l'intégration des systèmes, l'équipement de surveillance, la planification des mesures d'urgence en cas de catastrophe, etc. Un soutien indirect permettrait d'établir de nouveaux programmes d'études collégiales et universitaires axés sur les IE et les répercussions sur la société. » [traduction]
>
> - Participant virtuel

Nous avons interrogé les participants sur les types de mesures incitatives que les IE vitales pourraient recevoir en guise de compensation pour l'impact des exigences obligatoires. Les répondants ont proposé des subventions, des prêts sans intérêt, le partage des coûts, des incitatifs fiscaux, du financement pour la conformité réglementaire et des concessions réglementaires.

Les répondants ont aussi indiqué qu'une protection de responsabilité serait nécessaire pour les IE assujetties à toute obligation de déclaration. Les participants ont aussi suggéré la reconnaissance publique du propriétaire ou de l'exploitant pour sa conformité, ainsi que le droit préférentiel de soumission pour des contrats gouvernementaux.

Des répondants ont noté que certaines mesures de soutien gouvernemental leur permettraient de se conformer à la réglementation. Ces derniers ont identifié la communication de lignes directrices sur les normes et les obligations, l'aide à la planification de la gestion des urgences, l'obtention de soutien pour l'embauche de personnel aux compétences spécialisées (p. ex. soutien financier pour l'embauche d'experts en cybersécurité) et de la formation.

Enfin, quelques répondants ont souligné le besoin occasionnel d'appliquer des pénalités en cas de non-conformité réglementaire. Dans ce contexte, les pénalités suggérées s'agissaient notamment d'amendes, de la perte d'allégements fiscaux et de restrictions sur le droit de soumission du propriétaire et de l'exploitant pour des contrats gouvernementaux.

Glossaire

Approche de gestion tous risques : Processus consistant à déterminer, à analyser et à évaluer les risques suivant une approche tous risques. Une approche tous risques prend en compte tous les types de risques, qu'ils soient accidentels, intentionnels ou naturels.

Bien : Propriété ou ressource comme un immeuble, un équipement, une installation, une propriété intellectuelle, des documents ou des données ayant une valeur pour le propriétaire. Un pont, les données des patients d'un hôpital, les manuels d'exploitation d'une installation, un barrage hydroélectrique, un véhicule municipal et un pipeline sont des exemples de biens d'infrastructure essentiels.

Changements climatiques : Changements à long terme des conditions météorologiques moyennes d'une région, comme sa température typique, les précipitations et le vent. Cette évolution signifie que l'éventail des conditions attendues dans de nombreuses régions changera dans les prochaines décennies. Il y aura aussi des changements au chapitre des conditions extrêmes.

Cybersécurité : Désigne la protection de l'information numérique, ainsi que l'intégrité de l'infrastructure qui l'héberge et la transmet. Plus précisément, la cybersécurité comprend l'ensemble des technologies, les processus, les pratiques, les réponses et les mesures d'atténuation conçus pour protéger les réseaux, les ordinateurs, les programmes et les données contre les attaques, les dommages ou des accès non autorisés, afin d'en assurer la confidentialité, l'intégrité et la disponibilité.

Danger : Phénomène, événement physique ou activité humaine susceptible d'occasionner des pertes de vies humaines ou des blessures, des dommages aux biens, des perturbations sociales et économiques ou une dégradation de l'environnement. Un danger peut être naturel, intentionnel ou accidentel.

Désignation : Identification des biens ou des entités d'infrastructure essentielle, en fonction de différentes approches comme l'analyse des risques, l'évaluation de la criticité et l'application de critères transversaux et sectoriels. La désignation peut servir à différentes fins, comme la mise en œuvre d'obligations réglementaires pour la protection des infrastructures essentielles ou l'établissement d'un inventaire pour appuyer la gestion des risques et l'intervention en cas d'incident.

Essentiel : Qui a une importance décisive ou cruciale dans la réussite, l'échec ou l'existence de quelque chose. La criticité existe selon un continuum, certaines infrastructures étant plus essentielles ou importantes que d'autres. La criticité d'une infrastructure fait référence à l'importance relative en termes de conséquences que sa défaillance aurait sur la population et ses ressources vitales.

Évaluation des répercussions : Outil de planification et de prise de décisions utilisé pour évaluer les effets positifs et négatifs potentiels des projets proposés. L'évaluation des répercussions tient compte d'un large éventail de facteurs et propose des mesures pour atténuer les effets négatifs du projet. Elle tient également compte des composantes des programmes de suivi (pour les projets qui sont autorisés à aller de l'avant) qui vérifient l'exactitude d'une évaluation des répercussions et l'efficacité des mesures d'atténuation.

Forum national intersectoriel (FNI) : Réseau qui réunit des représentants de chacun des dix secteurs des infrastructures essentielles et des gouvernements fédéral, provinciaux et territoriaux afin d'établir les priorités, de discuter de problèmes intersectoriels et des interdépendances et de favoriser l'échange de renseignements et de pratiques exemplaires entre les secteurs. Le FNI se concentre sur les problèmes qui favorisent une approche tous risques de la gestion du risque en matière d'IE.

Gestion du risque : Approche systématique visant à établir la meilleure façon de procéder dans des circonstances incertaines par la détermination, l'évaluation, la compréhension, le règlement et la communication des questions liées aux risques. Elle fait partie intégrante des mécanismes d'une saine gestion.

Gouvernance : Système par lequel sont prises les décisions relatives au fonctionnement d'une organisation. Un système de gouvernance détermine comment les objectifs sont établis et atteints, comment les risques sont surveillés et gérés, et comment le rendement est optimisé.

Infrastructure communautaire : Comprend les structures, les lieux et les organisations qui soutiennent la vie quotidienne et le bien-être des résidents d'une collectivité. Les parcs locaux, les bibliothèques et les refuges pour sans-abri sont des exemples d'infrastructures communautaires.

Infrastructure essentielle (IE) : Comprend des processus, des systèmes, des installations, des technologies, des réseaux, des biens et des services qui sont nécessaires afin de garantir la santé, la sûreté, la sécurité et le bien-être économique

des Canadiens et des Canadiennes, ainsi que pour assurer le fonctionnement efficace des opérations du gouvernement. Il peut s'agir d'infrastructures indépendantes ou interconnectées et interdépendantes à l'intérieur des frontières du pays, d'une province ou d'un territoire ou entre ces endroits. La perturbation de ces infrastructures essentielles pourrait se traduire en pertes de vies et en effets économiques néfastes et pourrait considérablement ébranler la confiance du grand public. Les infrastructures essentielles comprennent les infrastructures physiques et numériques. L'infrastructure physique désigne l'environnement bâti, y compris les bâtiments, les véhicules, le matériel informatique et d'autres biens. L'infrastructure numérique désigne les systèmes et les biens électroniques, comme les données et les logiciels.

Infrastructure naturelle : Fait référence à l'utilisation de caractéristiques et de matériaux écosystémiques préservés, restaurés ou améliorés (p. ex. eau, végétation indigène, sable et pierre) pour produire des résultats en matière d'infrastructure et de services communautaires ciblés.

Institutions démocratiques : Règles, organisations, processus et systèmes qui sous-tendent un gouvernement responsable de représentants élus.

Interdépendance : Deux ou plusieurs choses, biens, systèmes ou personnes qui dépendent les uns des autres. Il existe des interdépendances au sein des secteurs des infrastructures essentielles et entre eux, ce qui signifie que les secteurs dépendent les uns des autres pour fournir des biens et des services essentiels aux Canadiens. La nature interdépendante des secteurs des infrastructures essentielles signifie que la défaillance d'un secteur peut avoir des répercussions sur d'autres secteurs.

Intersectoriel : Désigne plus d'un secteur et généralement les dix secteurs des infrastructures essentielles du Canada. Par exemple, le Forum national intersectoriel est un forum intersectoriel où sont représentés les dix secteurs des infrastructures essentielles.

Intervenant : Partie ou organisation ayant un intérêt, un rôle ou une responsabilité liée aux objectifs d'une autre organisation ou institution. Les intervenants qui participent au renouvellement de la Stratégie nationale sur les infrastructures essentielles comprennent globalement les gouvernements fédéral, provinciaux, territoriaux et autochtones, les administrations municipales, les propriétaires et exploitants d'infrastructures essentielles du secteur privé, ainsi que les universités et les groupes

de réflexion ayant une expertise en matière de sécurité et de résilience des infrastructures essentielles.

Menace : Situation dans laquelle il y a présence d'un aléa et d'une exposition à celui-ci. Les menaces peuvent être d'origine naturelle ou anthropique, et être accidentelles ou intentionnelles.

Ministère fédéral responsable : Ministère ou organisme fédéral chargé de favoriser l'échange de l'information et la collaboration au sein d'un secteur des infrastructures essentielles.

Position, navigation et synchronisation (PNS) : Les renseignements relatifs à la position, à la navigation et à la synchronisation sont utilisés pour comprendre où nous nous trouvons sur la surface de la Terre (position), pour déterminer comment nous rendre là où nous devons aller (navigation) et pour synchroniser les réseaux, ou pour l'horodatage (synchronisation). Les systèmes mondiaux de navigation par satellite (GNSS) sont largement utilisés pour fournir ces données précises en matière de PNS.

Processus : Actions ou mesures prises pour atteindre un résultat. Par exemple, le changement des feux de circulation suit un processus permettant aux véhicules de circuler.

Propriétaires et exploitants : Les entités publiques et privées qui possèdent, exploitent, entretiennent ou fournissent des biens, des systèmes et des services liés aux infrastructures essentielles.

Réseau multisectoriel : Réseau qui rassemble des représentants de niveau opérationnel de chacun des dix secteurs des infrastructures essentielles pour discuter de sujets liés à la résilience des infrastructures essentielles. Ces réunions annuelles permettent d'examiner les priorités canadiennes en matière d'infrastructures essentielles d'un point de vue intersectoriel et englobant plusieurs provinces et territoires, de faciliter l'échange en temps opportun de renseignements pertinents sur les risques liés aux infrastructures essentielles et les questions émergentes, et de favoriser les partenariats intersectoriels entre les propriétaires et les exploitants d'infrastructures essentielles.

Réseaux sectoriels : Réseaux dont le but est de permettre la discussion et l'échange de renseignements entre les intervenants de l'industrie et les gouvernements sur les

priorités du réseau sectoriel et les questions émergentes. Chaque réseau sectoriel est dirigé par un ministère ou un organisme du gouvernement fédéral, qui sont chargés de désigner les membres du réseau sectoriel. Par exemple, le ministère des Finances dirige un réseau du secteur des finances composé de représentants des principales institutions financières du Canada.

Résilience : Capacité d'un système, d'une collectivité ou d'une société à s'adapter au changement ou à une perturbation tout en maintenant un niveau acceptable de fonctionnement. Améliorer la résilience des infrastructures essentielles signifie améliorer la capacité de ces dernières à continuer de fournir aux Canadiens les biens, les services et les infrastructures dont ils ont besoin en cas de danger.

Risque : Combinaison de la possibilité qu'un aléa donné se produise et des conséquences potentielles pouvant y être associées. Le risque fait référence à la vulnérabilité, à la proximité ou à l'exposition aux dangers, ce qui influe sur la probabilité de répercussions indésirables.

Sécurité : Degré auquel une personne, une organisation ou une chose, comme une infrastructure, est à l'abri de toute atteinte ou perturbation intentionnelle, et capacité de continuer à fonctionner de manière fiable en toute sécurité. La sécurité peut également faire référence à l'intégrité et à la confidentialité des renseignements. Par exemple, des mesures de cybersécurité sont nécessaires pour protéger les données de recherche contre tout accès et toute manipulation non autorisée.

Gestion des urgences : Ensemble des activités et des mesures visant la gestion des risques de catastrophes de toute nature et couvrant les dimensions de la prévention, de l'atténuation, de la préparation, de l'intervention et du rétablissement.

Système : Plusieurs choses ou personnes qui interagissent pour remplir une fonction ou produire un résultat. Un système peut être relativement simple, comme le système logiciel de gestion de l'information d'une organisation, ou complexe, comme un système de contrôle industriel qui surveille la qualité de l'eau dans une installation de traitement des eaux.

Système mondial de navigation par satellite (GNSS) : Constellation de satellites qui fournissent des signaux de positionnement, de navigation et de synchronisation. Le système de positionnement global (GPS) est un exemple de GNSS.

Vulnérabilité : Conditions déterminées par des facteurs ou des processus physiques, sociaux, économiques et environnementaux qui accentuent la sensibilité de quelque chose aux effets des aléas. Elle représente en quelque sorte une mesure de l'état de préparation de l'infrastructure et à quel point cette dernière est outillée pour limiter les effets des aléas ou y faire face.