Rapport évolutif

Les infrastructures essentielles : un défi pour la sécurité des États

Monica Tremblay, M. Sc.
Anthropologue

Laboratoire d'étude
sur les politiques publiques
et la mondialisation

Analyse des impacts de la mondialisation sur la sécurité - Rapport 10
Juin 2011

ENAP
L'Université de l'administration publique

INTRODUCTION

La divulgation, en février dernier, d'attaques ciblant des infrastructures nucléaires iraniennes à l'aide d'un virus informatique et des réseaux informatiques du gouvernement fédéral canadien[1], confirme l'importance que doivent accorder les États et gouvernements à la protection des infrastructures essentielles. Les problèmes qu'éprouve actuellement le Japon à la suite de l'accident à la centrale nucléaire de Fukushima en sont un autre exemple éloquent. Trois événements, parmi un large éventail de risques qui illustrent la nécessité de la protection des infrastructures essentielles.

La mise en place de mesures de sécurité entourant les infrastructures essentielles d'un État ne constitue pas une nouveauté, mais la mondialisation et des facteurs qui y sont associés en redéfinissent tout de même les contours. Le développement des technologies de l'information et des communications, la déréglementation et l'ouverture des frontières ont favorisé la circulation de l'information, des biens et des personnes, ce qui a fait naître de nouveaux défis en matière de sécurité. Les tristes attaques de terrorisme international survenues, notamment depuis 2001, à New York, à Madrid, à Londres et à Mumbaï sont également venues rappeler l'existence de risques auxquels sont soumises différentes infrastructures et le besoin de les protéger et de les défendre selon les normes actuelles.

Ce rapport traite de l'impact de la mondialisation sur la protection des infrastructures essentielles. Après quelques précisions sur le type d'infrastructure dont il est question, on signale les principaux aspects dont il faut tenir compte afin de protéger les infrastructures essentielles et assurer la sécurité de la société. On jette ensuite un regard sur les mesures déployées par certains États en vue de sécuriser leurs infrastructures et de protéger la population. On examine enfin les aspects reliés à la mondialisation qui exercent des pressions en matière de protection des infrastructures essentielles.

1. LES INFRASTRUCTURES ESSENTIELLES, C'EST QUOI?

1.1 Définition générale et spécificités

De manière générale, on entend, par infrastructures essentielles[2], l'ensemble des établissements et des équipements « qui jouent un rôle crucial dans le fonctionnement de la société » et dont la paralysie ou la destruction « fragiliserait la sécurité nationale et compromettrait les intérêts économiques et sociaux d'un État » (Dunn Cavelty, 2007 :16). L'Organisation de coopération et de développement économiques (OCDE, 2008 : 2) précise qu'elles sont le « moyen d'assurer la fourniture de biens et services[3] nécessaires à la prospérité, à la croissance et à la qualité de vie, c'est-à-dire au bien-être, à la santé et à la sécurité des citoyens, ainsi qu'à la qualité de leur environnement ».

La définition d'infrastructure essentielle est, dans l'ensemble du monde, similaire. Certes les définitions sont nombreuses, mais il y a certaines constantes en ce qui a trait aux conséquences sur la population, l'économie et le gouvernement. Il existe cependant, selon les pays ou groupes régionaux, des nuances qui peuvent teinter les stratégies de protection adoptées et les différentes mesures mises en œuvre (Abele-Wigert et Dunn, 2006). Par exemple, le Canada inclut, dans les infrastructures, les processus et les services, dont des services gouvernementaux[4]; le Québec, pour sa part, insiste moins sur les aspects économiques[5]; la France, elle, insère,

dans sa définition, le risque de « mettre gravement en cause la santé ou la vie de la population » (Daguzan, 2010 :1005). L'Union européenne (UE) précise, dans sa définition, qu'il s'agit d'infrastructures « dont l'arrêt ou la destruction pourrait avoir une incidence grave sur deux ou plusieurs États membres ou un seul, s'il s'agit d'un État membre autre que celui dans lequel l'infrastructure critique est située » (Daguzan, 2010 : 1011)[6].

De plus, Abele-Wigert et Dunn (2006), dans un inventaire des politiques de protection des infrastructures d'information essentielles[7], signalent comment l'acception de « critique » varie, en outre, dans le temps et selon le contexte. Ainsi, au cours des années 1990, certains États ont accordé davantage d'importance à la protection des infrastructures d'informations essentielles, de par leur évolution et leur utilisation plus étendue et parce qu'elles se trouvent fréquemment à la base du fonctionnement d'autres infrastructures.

1.2 Identification des infrastructures essentielles

Une infrastructure est reconnue essentielle selon sa position stratégique parmi plusieurs infrastructures et spécialement en raison de son interdépendance avec les autres infrastructures. La plupart des États et groupes d'États, comme l'Union européenne, identifient les infrastructures essentielles, par secteurs. Le choix de secteurs a été inspiré par l'organisation des milieux d'affaires et de l'industrie. D'ailleurs, dans tous les pays, le secteur finance ou économie est toujours présent. Aussi, un grand nombre d'États[8] ont emboîté le pas à la Commission présidentielle de protection des infrastructures essentielles (PCCIP) des États-Unis, qui a été la première à identifier officiellement les infrastructures essentielles selon des secteurs d'affaires (Abele-Wigert et Dunn, 2006).

Selon Bruner et Suter (2008) qui ont dressé la mise à jour d'un inventaire des politiques de protection des infrastructures dans plusieurs pays et organisations internationales[9], les secteurs des banques et de la finance, des services gouvernementaux, des télécommunications et des technologies de l'information et des communications, des services d'urgence, de l'énergie et particulièrement de l'électricité, des soins de santé, des transports et de l'approvisionnement en eau sont le plus souvent identifiés.

Ces divisions sont modifiées au fil du temps. À la création, en 1996, du programme de protection des infrastructures essentielles aux États- Unis (PCCIP), huit secteurs étaient identifiés et ils s'élevaient à 18 en 2008 (Bruner et Suter, 2008). Au Québec et au Canada, après la tempête de verglas de 1998, on a identifié un sous-secteur essentiel : les services météorologiques[10]. On peut penser que le Japon enrichira sa liste d'un nouveau secteur après le séisme et le tsunami dévastateurs du mois de mars, de cette année. Selon l'International CIIP Handbook de 2006 et de 2008, le Japon n'avait pas identifié comme secteur ou sous-secteur essentiel, l'industrie chimique et nucléaire. Par contre, l'énergie et l'électricité y sont inscrites. Il est possible que les centrales nucléaires soient incluses

Inquiétudes suscitées par Wikileaks

La récente liste des sites que les États-Unis souhaitent protéger du terrorisme, révélée par WikiLeaks en décembre 2010, identifie précisément certaines infrastructures essentielles de divers pays, tels que des centrales de production d'énergie, des ponts et des tunnels, des entreprises pharmaceutiques, etc. (RC, 2010; Zetter, 2010). Pareille diffusion d'informations jugées secrètes a sonné l'alarme quant aux risques qu'elle peut entraîner. Des personnes mal intentionnées, terroristes ou pas, détiennent maintenant en quelque sorte une « liste d'épicerie ». Dans un rapport publié par l'OTAN, en 2007, était signalée la préoccupation face à « l'opportunité de dresser une liste concrète des infrastructures critiques européennes » (Jopling, 2007 :15), craignant qu'elle ne serve aussi les terroristes.

dans cette rubrique. Ce même pays avait ajouté les services médicaux en tant que secteur critique au moment où la grippe aviaire suscitait beaucoup de craintes.

2. LA PROTECTION DES INFRASTRUCTURES ESSENTIELLES

2.1 Pourquoi les protéger ?

Il est crucial, compte tenu du rôle que jouent les infrastructures essentielles dans la société, d'assurer leur fonctionnement et d'éviter une interruption qui pourrait avoir des répercussions importantes, entre autres, sur la sécurité de l'État et de la population à l'échelon local, puis international dans certains cas. La protection des infrastructures essentielles doit donc être une préoccupation constante. Selon différents spécialistes, il faudrait actuellement être plus vigilant, plus spécifiquement en ce qui concerne la cybersécurité et les infrastructures énergétiques : c'est ce que révèlent notamment, un rapport d'analyse des politiques et de la littérature scientifique d'un réseau de travail international sur la protection des infrastructures essentielles (CRN, 2009) et le rapport d'un consortium du National Homeland Security qui a établi les priorités des États-Unis en matière de sécurité (Hammond, 2011).

2.2 De quoi et de qui les protéger?

Les risques dont il faut protéger les infrastructures essentielles sont d'ordre divers et toutes n'en sont pas affectées de la même manière. Il existe bien sûr les catastrophes naturelles qui pourraient endommager ou interrompre le fonctionnement des infrastructures essentielles. Les accidents d'origine technique ou humaine, sont aussi à prévoir. Comme pour la sécurité informatique, les risques que représentent les employés sont à considérer, si on veut assurer une protection adéquate. Nul n'est à l'abri de l'erreur ou de la négligence. Enfin, depuis quelques années, on évoque fréquemment l'urgence d'envisager les possibilités d'attentats terroristes et d'actes criminels. Il faut, entre autres, prendre en compte les personnes ou groupes de personnes mal intentionnées qui souhaiteraient délibérément porter atteinte à une ou plusieurs infrastructures d'un État par différents moyens. D'aucuns expliquent que le terrorisme « n'est pas le [risque] le plus probable, ni le plus dangereux en termes de dégâts » (Dunn Cavelty 2007 :18). Toutefois, les infrastructures essentielles sont devenues des cibles éventuelles de la « guerre asymétrique », c'est-à-dire, de la confrontation indirecte d'ennemis à l'aide de moyens variés et avec divers acteurs, d'où la nécessité de hausser le degré de protection des infrastructures essentielles[11] contre le terrorisme. La Commission européenne souligne, dans un train de mesures sur la sécurité, que la menace terroriste est encore présente[12] et les États-Unis annonçaient, en février dernier, que le niveau d'alerte au terrorisme était plus élevé que jamais[13].

2.3 Des différences liées à la mondialisation

Une étude de l'influence de la mondialisation sur la sécurité de la société en Norvège explique que

> la mondialisation est un élément important dans le nouveau paysage [de la sécurité]. La Commission [norvégienne sur la vulnérabilité] soutenait d'ailleurs que la société est devenue plus vulnérable, en partie à cause de l'interdépendance et de la complexité des infrastructures essentielles, et parce que les crises et les catastrophes sont devenues mondiales [notre trad.] (Burgess et Jore, 2008: 3).

Cette citation illustre bien les principaux éléments qui ressortent de la documentation concernant la protection des infrastructures essentielles. Trois principaux facteurs associés à la mondialisation influencent le besoin et la manière de protéger ces infrastructures : la possibilité d'attaques terroristes, l'interdépendance et enfin, l'évolution des technologies de l'information et des communications avec, plus particulièrement, la montée en force des réseaux informatiques.

Terrorisme et contre-terrorisme

Le terrorisme international est un des risques auxquels sont exposées les infrastructures essentielles et auquel on pense spontanément, depuis le 11 septembre 2001. Les attentats subséquents en différents endroits de la planète et les mesures de contre-terrorisme déployées par les États ont aussi contribué à propager et à accentuer la crainte du terrorisme.

À l'opposé de la Guerre froide, où les menaces militaires pesaient principalement sur les infrastructures essentielles, actuellement les États sont davantage confrontés à des risques inattendus et incertains (Dunn, 2007). Dans ce climat, les pays se préparent moins pour la guerre qu'à consacrer leurs efforts à la sécurité de leur population. Dans un contexte où la menace n'est pas claire, plusieurs États, comme la Norvège, visent davantage à renforcer leur société afin qu'elle puisse faire face à différentes crises et diverses menaces, tant d'ordre naturel qu'humain, voire terroriste (Burgess et Jore, 2008).

Interdépendance des infrastructures essentielles

De nos jours, les infrastructures essentielles sont souvent interreliées entre elles et, dans bien des cas, interdépendantes et complémentaires. L'interdépendance entre les infrastructures essentielles est accrue par la mondialisation. Dans ce processus, de nouveaux marchés se sont développés et les réseaux se sont agrandis, grâce à la déréglementation et l'ouverture des frontières. Cela a contribué à allonger les chaînes d'offre de différentes ressources et a ainsi permis d'obtenir des services, tels que la fourniture d'électricité en provenance d'autres pays (OCDE, 2008). Une grande partie des infrastructures dépend aussi des systèmes de contrôle informatique qui servent à garantir la fiabilité de leur bon fonctionnement (Dunn Cavelty, 2007). Dans ce contexte, plusieurs secteurs dépendent l'un de l'autre. Il faut particulièrement considérer l'interdépendance entre les secteurs public et privé, puisque ce dernier est, depuis les années 1980, fréquemment propriétaire ou opérateur des infrastructures essentielles.

L'interdépendance facilite donc le fonctionnement des infrastructures et favorise l'offre de service à l'échelon local, national et international. Néanmoins, cette interdépendance se révèle aussi un maillon faible de la sécurité des infrastructures. Rares sont les documents qui ne font pas mention de la vulnérabilité accrue par l'interdépendance des infrastructures, et surtout en lien avec les infrastructures informationnelles. Une défaillance dans une infrastructure essentielle peut, par un effet de cascade, en affecter plusieurs autres (Renda et Hämmerli, 2010). Les chercheurs parlent alors de « l'effet domino »[14]. Au Québec, des spécialistes de la question travaillent, entre autres, à développer des modèles d'évaluation de l'interdépendance entre les infrastructures

afin d'aider à réduire la vulnérabilité des infrastructures essentielles[15]. Ils examinent particulièrement les effets d'interruption dans les systèmes de transports sur d'autres infrastructures essentielles.

Évolution technologique

L'évolution des technologies de l'information et des communications et particulièrement de l'informatique a modifié les façons de travailler et a accru les interrelations entre les systèmes. Miller (2009), professeur-chercheur de la National Defense University à Washington D.C. qui a aussi exercé des fonctions gouvernementales en matière de protection des infrastructures essentielles, énonce clairement comment les sociétés modernes sont devenues, sans le réaliser, dépendantes de toiles de réseaux extrêmement complexes et de systèmes étroitement couplés. Il souligne de plus, qu'en plus d'accroître la productivité de manière impressionnante :

> La mondialisation, les pratiques de juste à temps (JAT)[16] et le développement des systèmes de contrôle en réseau […] nous ont aussi exposés aux nouveaux dangers, encore partiellement compris, au fur et à mesure que des infrastructures sous-jacentes sont endommagées ou déconnectées. Ces infrastructures fonctionnent à une échelle nationale (ou mondiale), et requièrent des actions d'ensemble afin de les garder viables [notre trad.] (Miller, 2009 : 3).

Désormais, il n'est pas nécessaire qu'une information soit consignée là où une personne reçoit un bien ou un service. Les banques de données informatisées qui permettent de dispenser à distance des services bancaires et des services publics en sont un exemple. Les organisations peuvent donc avoir des ramifications à travers le monde. Cet avantage considérable a, par contre, augmenté les défis à sécuriser les différents systèmes et, par extension, les infrastructures essentielles. Une fuite d'informations dans un système peut avoir des effets négatifs en différents endroits de la planète. Les problèmes récents qu'a éprouvés Sony avec son réseau en nuage, le Play Station Network, illustrent bien comment des données sensibles interreliées ont été compromises et que cela affecte des usagers répartis partout dans le monde. Cet incident montre à quel point cette question est rapidement devenue une préoccupation planétaire. Il n'y avait pourtant rien d'essentiel dans ce service.

2.4 Qui est responsable de la protection?

La protection des infrastructures essentielles n'est pas seulement sous la responsabilité de ses propriétaires, administrateurs, ou opérateurs; les secteurs public et privé en sont conjointement responsables.

Les organisations internationales, dans le contexte actuel, jouent aussi un rôle dans la protection des infrastructures, par leurs ramifications multiples ou encore par l'influence qu'elles peuvent avoir à l'échelle de la planète (Daguzan, 2010). La plupart des organisations internationales, telles que l'ONU, l'OCDE, la Banque mondiale, l'OTAN et l'Organisation pour la sécurité et la coopération en Europe (OSCE), s'intéressent, de près ou de loin, à la protection des infrastructures essentielles. Certaines de ces organisations tentent d'ailleurs de développer des stratégies en fonction de secteurs particuliers; c'est le cas de l'OSCE dans le secteur énergétique (Daguzan, 2010).

2.5 Comment assurer le fonctionnement des infrastructures essentielles?

Afin de bien protéger les infrastructures essentielles, l'élaboration d'une stratégie de protection est incontournable. Des directives nationales sont émises à ce sujet dans plusieurs États et les responsables des infrastructures essentielles doivent planifier la protection. Il n'existe pas de solution universelle, étant donné que chaque infrastructure a ses particularités et qu'un éventail de risque est présent; c'est pourquoi les mesures de sécurité doivent être adaptées selon l'infrastructure. De nombreux textes soulignent que, dans le contexte de la mondialisation, l'interaction accrue entre les infrastructures et l'importance des systèmes informatiques sous-jacents au fonctionnement des infrastructures augmentent les risques d'origines diverses[17]. Ce qui fait dire à certains analystes de la question qu'il est préférable d'adopter une stratégie de protection en prévision de tous types de risques puisqu'ils sont trop nombreux et variés (Dunn Cavelty, 2007, 2010).

Il existe donc différentes approches dans le domaine de la gestion des risques et certaines orientations et tendances qui entrent en considération dans la protection des infrastructures essentielles.

Plus particulièrement depuis 2005, à la suite de la déclaration d'Hyogo, à l'issu de la Conférence mondiale sur la prévention des catastrophes [naturelles], les nouvelles stratégies et les plans de protection des infrastructures essentielles insistent sur la résilience. Cette approche exige d'appréhender la réalité autrement afin de définir le plan de protection (Dunn, 2007). On part ici de la prémisse qu'un problème surviendra et qu'il faudra être prêt et en mesure de rétablir l'infrastructure et les services afférents le plus rapidement possible afin d'éviter une série d'autres événements néfastes[18]. Avec cette approche, les responsables doivent planifier, entre autres par l'aménagement d'un environnement propice, la manière dont sera rétabli le service et comment reprendront les activités socio-économiques et politiques des communautés affectées.

La prochaine section offre un aperçu de mesures nationales et internationales établies au cours des 15 dernières années afin de sécuriser les infrastructures essentielles et signale certains changements survenus depuis le 11 septembre 2001 ou plus récemment.

3- MESURES DE PROTECTION EN AMÉRIQUE DU NORD ET DANS L'UNION EUROPÉENNE

3.1 Aux États-Unis

Les États-Unis ont été les premiers à se préoccuper considérablement des nouvelles vulnérabilités des infrastructures critiques (Dunn, 2007)[19]. Une Commission présidentielle sur la protection des infrastructures essentielles (PCCIP) a été mise en place, en juillet 1996. Elle devait, entre autres, identifier les menaces qui pesaient sur les infrastructures essentielles nationales, particulièrement en lien avec les réseaux informatiques et proposer une stratégie visant à protéger ces infrastructures. La Commission recommande, entre autres, l'élaboration d'un plan national et de plans sectoriels de protection des infrastructures, tant physiques qu'informatiques, dans des domaines vitaux, c'est-à-dire la sécurité nationale, la santé publique et l'économie. Elle souligne, de plus, qu'il s'agit d'une responsabilité que doivent partager les secteurs public et privé. N'ayant pas identifié de menaces criantes contre les

infrastructures physiques et craignant davantage les risques soulevés par un plus grand usage de l'informatique, la commission recommande d'accorder la priorité à la cybersécurité. Depuis les attaques du 11 septembre 2001, une plus grande attention est aussi portée à la protection des infrastructures essentielles physiques (Moteff, 2010).

Une directive présidentielle[20] encadre, depuis 1998, la protection des infrastructures essentielles des États-Unis. Conformément à celle-ci, les responsables de la protection des infrastructures essentielles nationales doivent assurer une gestion active des risques et œuvrer à l'amélioration de la planification de la sécurité (Daguzan, 2010). Cette directive désigne les différents secteurs où se trouvent des infrastructures essentielles à protéger[21]. Elle met aussi en place une structure de gestion composée de plusieurs comités et définit la responsabilité des différents acteurs, y compris du secteur privé. On encourage notamment celui-ci à se doter d'un centre d'analyse et de partage de l'information, particulièrement en matière de cybersécurité (Moteff, 2010).

À l'arrivée de l'administration Bush, certains changements ont été apportés à la structure de gestion; les activités de protection des infrastructures essentielles sont confiées à un comité de coordination des politiques (PCC) responsable du contre-terrorisme et de la préparation nationale. Après les attaques du 11 septembre 2001, le Président Bush crée l'Office of Homeland Security qui, selon la Stratégie nationale de sécurité intérieure, doit, entre autres, protéger les États-Unis et ses infrastructures essentielles des conséquences d'attaques terroristes. En plus des mesures de protection, ce bureau a, parmi ses fonctions, la responsabilité de « coordonner les efforts visant à assurer le rétablissement rapide des infrastructures essentielles après une interruption par une menace ou une attaque terroriste » [notre trad.] (Moteff, 2010 : 9). On voit ici poindre l'intérêt pour la résilience.

En 2002, une Stratégie nationale de protection des infrastructures essentielles physiques et des ressources clés[22] est élaborée. C'est le Department of Homeland Security (DHS) qui, conformément à sa loi constitutive de 2002, dirige et coordonne les efforts de protection des infrastructures essentielles de toute la nation. Le DHS a aussi l'autorité d'identifier de nouveaux secteurs où se trouvent des infrastructures essentielles (GAO, 2010 : 2). Chacun des secteurs est, de plus, piloté par une organisation (leading agency) spécifiquement désignée à cette fin. Ces agences sont responsables de la coordination des travaux entre les paliers gouvernementaux et avec le secteur privé (Jopling, 2007).

Le DHS, en tant que responsable de la coordination du développement et du maintien du plan national de protection des infrastructures essentielles, a déposé son premier plan national de protection des infrastructures (NIPP) en juin 2006 et en a proposé une mise à jour, en 2009. Dans cette dernière version, on met l'accent sur la résilience. Cet aspect a d'abord été identifié par le DHS, dans un rapport quadriennal sur la sécurité nationale, comme l'un des trois concepts essentiels d'une approche globale de la sécurité nationale (GAO, 2010 :13). Néanmoins, il semble que davantage d'efforts soient nécessaires afin d'opérationnaliser cet objectif. Dans une évaluation, réalisée entre août 2008 et septembre 2010, le Government Accountability Office (GAO) recommande au DHS de développer des mesures de performance de résilience. Il suggère aussi de mettre à jour le Protective Security Advisor Guidelines (PSA)[23] et d'évaluer la faisabilité de développer une stratégie visant la diffusion de l'information sur la résilience (GAO, 2010).

Bien que les États-Unis se préoccupent des risques de terrorisme international, ils ne négligent pas pour autant la possibilité de risques internes accrus par l'interdépendance des infrastructures. Le National Infrastructure Advisory Council (NIAC)[24] s'est penché sur la question et explique, dans un rapport sur la « menace interne aux infrastructures essentielles », comment la mondialisation peut être mise en cause devant la complexité croissante à protéger ces infrastructures. Il est fréquent qu'une infrastructure possède des ramifications dans différents pays. La gestion en matière de sécurité s'avère alors plus difficile, notamment par la quantité d'employés gravitant autour des infrastructures essentielles (NIAC, 2008).

3.2 Au Canada

Dans le contexte international de crainte du terrorisme qui s'installe en 2001, le Canada entreprend de mettre en place des politiques de protection des infrastructures essentielles, tant matérielles qu'informationnelles. En 2003, le gouvernement réunit différents ministères et organismes qui ont des responsabilités en matière de protection des infrastructures et de sécurité civile au sein du ministère de la Sécurité publique et de la préparation aux urgences, aujourd'hui Sécurité publique Canada. Ce ministère a alors le mandat de protéger la population des nombreux risques auxquels elle peut être exposée, tant naturels que criminels et terroristes. Ce ministère travaille, dès sa création, au développement d'une stratégie concertée en matière de protection des infrastructures essentielles. Comme d'autres pays, le Canada décide, en 2005, d'accorder davantage d'importance à la résilience dans la protection des infrastructures essentielles.

En 2007, on remplace la Loi sur la préparation aux urgences de 1985 par la Loi sur la gestion des urgences qui renforce le rôle du gouvernement fédéral sur la protection des infrastructures essentielles. « Elle confère au ministre de la Sécurité publique la responsabilité d'assurer un leadership à l'échelle nationale et d'établir une orientation claire concernant la gestion des urgences et la protection des infrastructures essentielles au sein du gouvernement du Canada » (Sécurité publique Canada, 2009).

En 2009, le Canada publie sa Stratégie nationale sur les infrastructures essentielles, coordonnée par Sécurité publique Canada. La stratégie identifie 10 secteurs d'infrastructures essentielles qui sont étroitement liés et interdépendants. Quel que soit le secteur, la priorité est accordée à la protection des infrastructures matérielles et informatiques. Il s'agit d'un « domaine de mission qui vise à édifier des capacités propres à renforcer et à soutenir la robustesse, la fiabilité, la résilience et la protection d'installations, de réseaux, de services et de biens matériels et informatiques qui, s'ils étaient perturbés ou détruits, pourraient avoir des effets graves sur la santé, la sécurité, l'économie ou le fonctionnement du pays[25] » (RDDC, 2010). Ainsi, « la Stratégie nationale et le plan d'action sur les infrastructures essentielles mettent en place une approche de gestion tous risques ». À l'aide de celles-ci, on souhaite accroître la résilience des biens et des systèmes intégrés « tels que l'alimentation, les réseaux électriques, transports, communications, et systèmes de sécurité publique » (Sécurité publique Canada, 2010).

Afin d'améliorer la coopération entre les acteurs concernés par les infrastructures essentielles des divers secteurs, le Programme technique de sécurité publique (PTSP) a créé une communauté de praticiens en protection des infrastructures

essentielles (CP PIE). Ce forum vise à améliorer la compréhension de l'interdépendance des infrastructures et à favoriser les interactions entre les différents acteurs. Il s'efforce de réunir des ministères et organismes fédéraux clés, des partenaires des provinces et des territoires et du secteur privé. Sont aussi invités des membres de la communauté des sciences et de la technologie du gouvernement, de l'industrie et du milieu universitaire. Ensemble, ils veillent à ce que les efforts de travail portent sur les domaines prioritaires permettant « de conserver la robustesse et la résistance des infrastructures essentielles du Canada » (CSS, 2010 : 5). De manière générale, un ministère est chargé de coordonner les activités du secteur qui le concerne plus spécifiquement.

Comme dans bien des pays, les mesures déployées oscillent entre la protection des infrastructures physiques et la sécurisation des infrastructures d'informations connectées au cyberespace. À l'automne 2010, le gouvernement du Canada a lancé une stratégie de cybersécurité afin que la GRC œuvre à la préparation d'une riposte contre les cybermenaces pouvant affecter les infrastructures essentielles et la sécurité nationale[26]. Cette stratégie identifie trois secteurs d'où peuvent provenir les menaces : les activités militaires ou étatiques d'espionnage, les attaques terroristes et le cybercrime. La mise en œuvre de cette stratégie est basée sur la coopération du secteur privé concerné par la protection des infrastructures essentielles ainsi que celle des autres paliers gouvernementaux (Thatcher, 2011a).

Le Canada coopère aussi avec les États-Unis en matière de protection des infrastructures essentielles. Les deux gouvernements fédéraux ont opté pour une coopération transfrontalière et ont établi un Plan d'action canado-américain sur les infrastructures essentielles. Ce plan vise principalement à « renforcer la résilience des infrastructures essentielles » à l'aide d'une approche intégrée et en intensifiant la coordination des activités et en encourageant le dialogue permanent entre les intervenants de part et d'autre de la frontière (Sécurité publique Canada, 2010a).

> Compte tenu des raffineries, des installations nucléaires, des grands services de fabrication et d'autres infrastructures à proximité de la frontière, ainsi que de l'énergie, de l'approvisionnement de services essentiels et des réseaux de transport traversant la frontière, les répercussions des perturbations franchissent les limites des administrations internationales. En raison de l'inter-connectivité de nos infrastructures essentielles, nos deux administrations doivent collaborer pour gérer les risques, au moyen de processus conjoints de planification, d'échange d'information et de tenue d'exercices visant à évaluer et à renforcer les plans en place (Sécurité publique Canada, 2010a).

3.3 Au Québec

Le Québec participe à la Stratégie nationale sur les infrastructures essentielles du Canada. La protection des infrastructures essentielles au Québec est, entre autres, sous la responsabilité du ministère de la Sécurité publique, qui a élaboré et mis en place le Plan national de sécurité civile, comme le commande la Loi sur la sécurité civile, adoptée en 2001. « La sûreté des infrastructures stratégiques du Québec constitue un enjeu incontournable en matière de sécurité de l'État et fait partie des préoccupations du ministère de Sécurité publique » peut-on lire sur le site de ce ministère[27].

En prévision d'éventuels actes malveillants, différentes initiatives en matière de protection des infrastructures essentielles ont été lancées au Québec, particulièrement

au sein du ministère de la Sécurité publique. Par exemple, on a identifié, évalué et localisé les infrastructures jugées prioritaires selon « leur degré d'importance pour la société québécoise » dans le cadre du Programme de sûreté des infrastructures prioritaires. Ce programme vise aussi à favoriser l'échange de renseignements concernant les menaces intentionnelles telles que le terrorisme. Cet objectif s'est traduit par la création, en 2008, d'un forum de représentants policiers et responsables d'infrastructures afin de faciliter l'échange d'information et la coordination des mesures de protection des infrastructures, le Groupe intégré sur la sûreté des infrastructures (GISI), coordonné par la Direction de la sécurité de l'État (DSE)[28] (Sécurité publique Québec, 2010). La DSE a, quant à elle, été créée en 2005, avec le mandat « d'informer et de conseiller les autorités ministérielles concernées à l'égard du terrorisme et des autres menaces susceptibles de déstabiliser ou de porter atteinte à la sécurité de l'État québécois, ainsi qu'au sujet des mesures visant à les contrer » (Sécurité publique Québec, 2010a). C'est cette direction qui a élaboré le Programme de sûreté des infrastructures prioritaires.

Les initiatives du ministère dans la lutte contre le terrorisme l'ont aussi amené à mettre en place, en 2006, le Centre de gestion de l'information de sécurité (CGIS), au sein de la DES. Ce centre a comme mandat d'éclairer le gouvernement du Québec sur « l'environnement de sécurité dans lequel il évolue ». Il traite donc « l'information relative aux menaces à la sécurité de l'État » (Sécurité publique Québec, 2009).

D'autres ministères et organismes sont concernés par la protection des infrastructures essentielles au Québec. La place que lui accorde le ministère des Relations internationales dans la Politique internationale du Québec évoque à quel point les infrastructures nationales s'inscrivent dans un ensemble plus vaste. L'interdépendance des infrastructures essentielles affecte aussi le Québec et vient rappeler la pertinence de la coopération internationale en matière de sécurité, particulièrement des infrastructures. Une des priorités du Québec et du continent nord-américain, mentionnée dans la Politique internationale du Québec (2006 : 77), consiste à « renforcer la sécurité des infrastructures stratégiques du Québec », notamment les « infrastructures publiques d'énergie électrique et des approvisionnements du Québec en hydrocarbures ». S'ajoute à cela, la « collaboration avec les États-Unis et certains pays européens sur la sécurisation des systèmes informatiques publics et la protection des renseignements personnels ».

Plusieurs autres ministères et organismes québécois se préoccupent de la protection des infrastructures essentielles. Dix-sept d'entre eux participent, notamment, à un projet d'évaluation de la résilience organisationnelle en collaboration avec le Centre risque et performance, de l'École Polytechnique de Montréal. Cette collaboration s'inscrit dans la foulée d'une démarche gouvernementale lancée en 2008 visant à « accroître la résilience de ses systèmes essentiels » (Neault, 2009). On aspire aussi mobiliser les propriétaires et les exploitants des infrastructures essentielles, privées ou publiques, à établir des partenariats et assurer la cohérence et la complémentarité des mesures à mettre en œuvre (Robert, Hémond et Yan, 2010).

3.4 Dans l'Union européenne

Comme dans plusieurs autres États du monde, la propriété ou l'opération de plusieurs infrastructures ont été privatisées et déréglementées en Europe. Après l'attaque de Madrid en 2004, le Conseil européen demande la préparation d'une stratégie d'ensemble de la protection des infrastructures essentielles. À partir de ce moment, la Commission européenne adoptera différentes directives et communications afin de protéger les infrastructures essentielles, plus spécifiquement contre le terrorisme. En décembre 2004, naît l'idée de préparer un Programme européen pour la protection des infrastructures essentielles (EPCIP[29]) et la nécessité d'instaurer un réseau dédié au soutien de cette activité, le Critical Infrastructure Warning Information Network (CIWIN[30]). Dès lors, plusieurs actions visant à intégrer les politiques de protection des infrastructures essentielles seront entreprises. Notons la définition d'un partenariat public-privé européen pour la résilience (EP3R) et le Forum européen des États membres.

En novembre 2005, un livre vert sur la protection des infrastructures essentielles est publié. On y signale les problèmes auxquels le Programme de protection devra s'attaquer et on y définit ce que sont les infrastructures essentielles et les onze secteurs qui les regroupent. L'objectif principal de la protection des infrastructures essentielles dans les États membres consiste à assurer un niveau de protection adéquat et une reprise rapide du fonctionnement dans l'Union européenne (Svedin, 2009). À la base, chaque État reste maître de ses infrastructures nationales, mais dans un cadre de protection commun à l'Union européenne.

En 2006, une communication de la Commission européenne définit les principes, les processus et des instruments permettant d'implanter le programme européen EPCIP. Ce programme devra servir à établir des procédures communes de recensement, de classement des infrastructures essentielles dans les États de l'Union et une structure permettant d'évaluer le besoin de renforcer leur protection (Daguzan, 2010).

Le EP3R est, quant à lui, encore à l'étape de la préparation. Outre son objectif principal d'améliorer le partage des informations entre les secteurs public et privé, ses objectifs et l'étendue de ses actions sont en cours d'élaboration. La création de ce partenariat s'est d'abord inscrite dans les mesures de protection des infrastructures informationnelles essentielles qu'on avait tendance à traiter séparément en Union européenne. Le Forum européen des États membres doit aussi servir à améliorer le partage d'informations afin de mieux sécuriser les infrastructures.

Parmi les autres actions, la Commission européenne travaille à accroître la coopération internationale en matière de protection des infrastructures essentielles au niveau mondial. Dans cette optique, elle collabore principalement avec les États-Unis, le Canada et le Japon afin d'identifier des principes et d'élaborer des lignes directrices qui pourraient être utilisés mondialement. Une difficulté importante se pose dans ce projet, car tous les États ne reconnaissent pas les mêmes infrastructures essentielles, dont l'Internet. Le Centre for European Policy Studies (CEPS) signale, dans un rapport sur la protection des infrastructures essentielles en Union européenne, publié en décembre 2010, ce même problème et trois autres qui mettent des embûches à l'amélioration transfrontalière et internationale de la sécurité dans ce domaine. D'abord, les États n'ont pas tous atteint le même niveau

en matière de protection des infrastructures essentielles. De plus, il existe une certaine coopération entre des États, malgré l'absence d'opérations chapeautées à l'échelon européen. Enfin, les partenariats avec le secteur privé se définissent au cas par cas, dans chaque pays.

4 – DÉFIS ACTUELS DE PROTECTION DES INFRASTRUCTURES ESSENTIELLES

À la lumière des écrits disponibles et des politiques élaborées afin de protéger les infrastructures essentielles, il apparaît qu'il s'agit d'un processus dynamique qui requiert une amélioration continue. La recherche de moyens permettant de mieux protéger les infrastructures, la population et son environnement, ainsi que la quête d'outils en vue d'évaluer les risques et les mesures déployées afin de répondre, le cas échéant, à une catastrophe, révèlent la nécessité d'un examen continu. Quelques préoccupations se démarquent particulièrement : le besoin d'adapter les approches de protection, la nécessité de composer efficacement avec l'interdépendance et l'intérêt de coopérer.

4.1 S'adapter à l'incertitude des risques ou la recherche de la résilience

Jusqu'à tout récemment, la protection des infrastructures reposait surtout sur une approche de gestion des risques qui demande d'anticiper des menaces précises et de développer des stratégies de réponse à celles-ci en réduisant les vulnérabilités du système, voire de l'infrastructure à protéger, et ainsi éviter ou atténuer les risques (Dunn Cavelty, 2010). Compte tenu de la méconnaissance de plus en plus grande des menaces et des impacts qui les accompagnent et qui pèsent sur les infrastructures, l'approche tend à changer. Deux tendances semblent cohabiter: l'une consiste à « limiter les risques en réduisant les vulnérabilités », l'autre, plus récente, consiste à aborder cette difficulté en « passant du concept de protection à celui de résilience » [notre trad.]. Il s'agit donc de travailler sur les conditions et réponses « post interruption » plutôt que sur des activités « pré interruption » visant à réduire les pertes potentielles par l'atténuation des dégâts éventuels (Dunn Cavelty, 2010 : 2-3).

La recherche de résilience dans les stratégies nationales apparaît être une tendance importante en matière de protection des infrastructures essentielles. En plus de prévenir les risques et réduire les vulnérabilités, les États font des efforts afin de préparer les infrastructures essentielles à pouvoir assumer leur rôle le plus rapidement possible à la suite d'une défaillance ou d'une interruption. On vise ainsi à interrompre le moins longtemps possible les activités quotidiennes de la population et de l'État.

4.2 Le besoin de coopération et l'urgence du partage d'information

Même si le secteur privé est souvent propriétaire ou responsable des infrastructures essentielles, les États, agissent en tant que régulateurs et consommateurs et sont responsables d'assurer la sécurité de leurs citoyens et le fonctionnement de la société. C'est pourquoi il devient incontournable pour ces deux secteurs de coopérer, entre autres, en matière de partage d'informations, afin de protéger adéquatement les infrastructures essentielles. Bruner et Suter (2008 : 535) expliquent que tous les États reconnaissent l'importance d'une telle coopération. Le partage d'information fait partie de cette coopération. De plus,

> les fournisseurs et utilisateurs des infrastructures essentielles doivent être sensibilisés à la menace. Par-dessus tout, nous avons besoin de comprendre que l'industrie, le gouvernement et les chercheurs ont tous un rôle à jouer dans la protection des infrastructures essentielles [notre trad.].

Les organisations internationales reconnaissent aussi l'importance de la coopération en matière de protection des infrastructures essentielles. Dans une de ses publications, l'OTAN (2007) soutient notamment, à quel point la coopération entre les secteurs public et privé est indispensable « compte tenu de la multiplicité d'acteurs aux intérêts divers ». Le rapport précise qu'un partenariat entre ces secteurs requiert du secteur privé qu'il s'engage à contribuer à l'atteinte des objectifs nationaux de sécurité. Quant au secteur public, il doit, en contrepartie, voir à une « répartition équitable des coûts inhérents aux mesures de protection » (Jopling, 2007 : 15).

Dans le but de faciliter la coopération avec le privé, le Canada a, par exemple, misé sur la division des infrastructures essentielles selon les secteurs de l'industrie et créé une table intersectorielle permettant aux responsables de chacun des secteurs de se réunir et discuter avec des représentants gouvernementaux. On tente ainsi d'éviter la multiplication des mécanismes de consultation, explique le responsable de la stratégie canadienne de cybersécurité (Thatcher, 2011).

Il existe néanmoins des contraintes à la coopération entre le gouvernement et le secteur privé. D'abord, l'écart d'expertise entre les acteurs privés et les organismes de régulation gouvernementaux complique parfois le développement des politiques. De plus, le secteur privé n'a pas tendance à partager les informations de crainte qu'elles deviennent publiques. Enfin, l'entreprise privée résiste parfois à investir dans l'amélioration de la sécurité des infrastructures qui, de son point de vue, est adéquate, et vise seulement dans ce contexte à respecter les standards gouvernementaux de sécurité publique. Selon les pays, d'autres difficultés compliquent aussi la coopération (Svedin, 2009).

Selon Dunn et Suter (2009), la coopération demeure incontournable et ne doit pas seulement être reliée au partenariat public-privé, elle doit être envisagée de toutes les manières possibles. Compte tenu de la place qu'occupe le secteur privé dans le domaine des infrastructures essentielles, le rôle du gouvernement devrait consister davantage à coordonner des réseaux d'auto-régulation et d'auto-organisation et à choisir les outils qui peuvent servir à motiver ces réseaux dans la protection des infrastructures essentielles. Dans ce cas, le rôle du gouvernement ne consiste plus à exercer une surveillance serrée, ni un contrôle immédiat. Les politiques reposeraient plutôt sur les réseaux d'auto-organisation.

La coopération doit aussi exister entre les différents paliers gouvernementaux; l'exemple du Canada et du Québec et celui des mesures auxquelles travaille l'Union européenne l'ont notamment montré.

4.3 S'adapter à l'interdépendance requiert aussi la coopération

Compte tenu des risques qui se mondialisent, comme le terrorisme et le crime, les changements climatiques qui affectent toute la planète, certains États, dont la Norvège, reconnaissent leur dépendance envers les autres et, par le fait même, le besoin de coopération à l'échelon international. Les crises qui surviennent à un endroit peuvent avoir des conséquences à l'étranger ou nécessiter les ressources d'un autre pays afin d'être surmontées (Burgess et Jore, 2008).

Plusieurs infrastructures essentielles sont déployées de part et d'autre des frontières nationales. L'interdépendance entre certaines accroît notamment le besoin de coopération internationale en matière de protection (Miller, 2009). La coopération internationale, liée à la protection des infrastructures essentielles, s'avère néanmoins plus difficile, particulièrement dans le secteur des systèmes d'information. Dans un contexte où les informations électroniques peuvent circuler et traverser les frontières facilement, il peut s'avérer difficile pour les États de trouver l'équilibre entre le partage de données et leur protection.

L'interdépendance des infrastructures essentielles requiert d'identifier là où des actions conjointes sont nécessaires. Le besoin d'avoir des plans et des approches qui en tiennent compte est désormais incontournable.

CONCLUSION

Ce rapport jette un regard sur la protection des infrastructures jugées essentielles dans de nombreux États. Il montre comment leur désignation et l'élaboration des stratégies de protection de ce type d'infrastructure préoccupent les responsables de la sécurité civile et il fait ressortir l'influence de la mondialisation en matière de protection des infrastructures. L'évolution des technologies de l'information et des communications et l'étendue des réseaux ont d'ailleurs modifié le contexte actuel, les cyberattaques font partie des risques à considérer, sans oublier l'interdépendance qui existe entre plusieurs systèmes informatiques et d'autres infrastructures. L'interdépendance en matière d'économie sur les marchés mondiaux joue aussi un rôle dans l'identification des infrastructures essentielles et dans le niveau d'interdépendance qu'elles ont entre elles, à l'échelon national et international. Après le 11 septembre, les risques de terrorisme sont venus hanter les États où on a travaillé à ajuster les plans de protection des infrastructures essentielles en se préoccupant davantage de ce type de risques. Au chapitre des catastrophes naturelles, l'ouragan Katrina, qui a frappé les États-Unis en 2005, a rappelé que d'autres éléments de protection devaient être pris en compte, notamment en matière de rétablissement du fonctionnement de la société.

Les politiques mises en place sont donc évaluées périodiquement, selon les événements qui surviennent dans le monde. L'Allemagne, notamment, revoit sa politique sur le nucléaire et réfléchit à la possibilité de fermer des centrales nucléaires à la lumière de la crise japonaise de mars 2011. Elle annonce fin mai que les centrales seront arrêtées d'ici 2022. Petit à petit, d'autres États emboîtent le pas dans une réflexion sur le nucléaire quant aux risques pour la sécurité de la population. Les responsables de la centrale nucléaire Fukushima-Daiichi ne parvenaient pas, un mois après le séisme, à reprendre le contrôle de la situation, ni à réduire les impacts sur l'environnement.

Cet exemple permet de souligner la tendance actuelle en matière de protection des infrastructures essentielles de planifier le rétablissement des services, en plus de la prévention et de la réduction des vulnérabilités des infrastructures. Compte tenu de l'étendue des risques, d'ordre naturel et humain, de l'aspect asymétrique des dangers d'attaques terroristes, de l'interdépendance des infrastructures et de l'étendue des réseaux, tous des aspects fortement reliés à la mondialisation, les États ne peuvent pas tout protéger, ni contre tout. Ils se préparent plutôt à limiter les dégâts et à reprendre les activités normales le plus rapidement possible.

Notes

1 La BBC signalait, le 15 février 2011, que des infrastructures industrielles, en lien avec le programme nucléaire iranien, ont été la cible du vers informatique « Stuxnet » qui aurait perturbé le fonctionnement normal de cette industrie. Le 16 février 2011, Radio-Canada annonçait que des cyber-pirates auraient réussi à infiltrer certains réseaux informatiques du Conseil du Trésor et du ministère des Finances du gouvernement canadien au cours des trois derniers mois.

2 On relève différentes appellations, dont infrastructures critiques, inspiré de l'anglais « critical infrastructures (CI) ». D'autres utilisent infrastructures vitales, notamment en France, et infrastructures stratégiques. Ce texte privilégie le terme d'infrastructures essentielles, reconnu par le bureau de la traduction du Canada comme l'équivalent de CI.

3 Robert, Wagner et Hémond, 2008, parlent plutôt d'un « ensemble de ressources » qui incluent les bien et services que fournissent les infrastructures essentielles.

4 La stratégie nationale sur les infrastructures essentielles les définit comme étant :

> *l'ensemble 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 et en effets économiques néfastes, et pourrait considérablement ébranler la confiance du grand public (Sécurité publique Canada, 2009a :2).*

5 Selon le ministère de la Sécurité publique du Québec une « infrastructure stratégique » est :

> *une infrastructure qui fournit un service d'une importance telle pour la société que sa perte engendrerait des conséquences majeures sur la santé, la sécurité ou le bien-être des citoyens ou encore sur le fonctionnement efficace du gouvernement. Une infrastructure peut prendre la forme d'une installation, d'un système, d'un réseau ou encore d'un bien (Sécurité publique Québec, 2010).*

6 Définition de ce que la Commission européenne appelle ICE - Infrastructure critiques européennes, cité dans Daguzan, 2010.

7 Il s'agit de systèmes d'information électroniques qui soutiennent le fonctionnement d'autres infrastructures essentielles. Les infrastructures d'information essentielles sont souvent perçues comme un sous-ensemble des infrastructures essentielles.

8 Les 25 États examinés dans les études du Center for Security Studies de Zurich, utilisent tous cette classification.

9 La première édition de ce document du Center for Security Studies du Swiss Federal Institute of Technology Zurich qui examine une série d'inventaires internationaux sur les politiques de protection des infrastructures d'informations essentielles a été réalisée par Abele-Wigert et Dunn en 2006.

10 Sécurité publique Canada publie un résumé quotidien sur les infrastructures. Des liens vers des infrastructures essentielles, voire des services gouvernementaux, sont disponibles (Sécurité publique Canada. 2011a. DIR11-100 - 26 mai 2011 : Liens utiles http://www.securitepublique.gc.ca/dir/dir11-100-fra.aspx?rss=false). Voir plus spécifiquement Environnement Canada. 2011. Avertissements météo publics pour le Canada : Programme d'alertes à la population, 13 avril. http://www.ec.gc.ca/meteo-weather/default.asp?lang=Fr&n=C9A8D735-1

11 Burgess et Jore, 2008, qui s'intéressent à l'influence de la mondialisation sur les mesures de sécurité en Norvège soulignent que les autorités norvégiennes considèrent le risque d'incident terroriste comme faible. Néanmoins, compte tenu de la perception de cette menace dans la société, des mesures de prévention du terrorisme sont déployées nationalement et internationalement.

12 Cité dans Coursaget, Alain. 2010 :6 qui présente un bilan du Secrétariat général de la défense et de la sécurité nationale des « activités d'importances vitales » en France.

13 Déclaration de Janet Napolitano devant la commission de la Sécurité intérieure de la Chambre des représentants, rapporté par Radio-Canada, le 9 février 2011.

14 Les travaux du Centre Risque et Performance (CRP) de l'École polytechnique de Montréal, traitent en profondeur de ce sujet. L'article de Robert et Morabito intitulé « Les effets domino » en trace les grandes lignes. Hémond et Robert (2010), quant à eux, examinent plus particulièrement la question à l'aide de l'exemple du système routier.

15 Voir les travaux de Benoît Robert et Luciano Morabito. Ces auteurs ont, entre autres, publié un guide méthodologique sur la réduction des vulnérabilités des infrastructures essentielles et travaillent à la modélisation de l'interdépendance des infrastructures essentielles.

16 On fait ici allusion à la méthode, développé chez Toyota, visant à rendre disponible au bon moment et en quantité suffisante ce qui est nécessaire à la production d'un bien ou d'un service. Cette forme d'organisation et de gestion est aussi appelée flux tendu. Voir : Inbound logistics Glossary. 2011. Just-in-Time Logistics (or Quick Response), http://www.inboundlogistics.com/glossary/j.shtml); Agence nationale pour l'amélioration des conditions de travail. 2007. Fiche pratique « Le flux tendu » © Réseau Anact http://www.anact.fr/portal/pls/portal/docs/1/304329.PDF.

17 Soulignent notamment cette réalité une publication sur la Protection des infrastructures critiques du Centre de politique de sécurité internationale du département fédéral des affaires étrangères de la Suisse, les textes de Jopling, 2007, de Burgess and Jore, 2008 et de Svedin, 2009.

18 Pour une compréhension en profondeur du concept de résilience en lien avec les infrastructures essentielles, voir le texte de Marie-Christine Therrien, 2010, « Stratégie de résilience et infrastructures essentielles » publiés dans un numéro sur La gestion des risques de la revue Télescope. Voir aussi l'application de la résilience dans les organisations responsables d'infrastructures essentielles dans les textes de Robert, B., Y, Hémond et G. Yan. 2010, « L'évaluation de la résilience organisationnelle » ou le document plus détaillé de Robert, B. et al., du Centre risque et performance, Résilience organisationnelle – Concepts et méthodologie d'évaluation, publié en 2009 http://www.polymtl.ca/crp/doc/Resilience-organisationnelle-Final_001.pdf

19 Il faut savoir qu'aux États-Unis, la majorité des infrastructures essentielles appartiennent au secteur privé. Lord Jopling, dans un rapport de commission de l'OTAN (2007), estime que plus de 85% des infrastructures essentielles sont détenues et exploitées par ce secteur. Les responsables de la PIC dans ce pays, reconnaissent de ce fait le besoin de coopération entre le secteur privé et le secteur public afin de mieux protéger les « avoirs et les systèmes » (GAO, 2010).

20 La Presidential Decision Directive 63 on Critical Infrastructure Protection – PDD-63

21 Aujourd'hui, 18 secteurs regroupent les infrastructures essentielles et les ressources clés.

22 National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.

23 Les Protective Security Advisors (PSAs) sont des experts formés en matière de protection des infrastructures essentielles et en atténuation des vulnérabilités. Ils sont notamment autorisés à visiter des infrastructures et à fournir des informations et des conseils en matière de protection. Les lignes directrices servent à faciliter le développement de liens entre eux et le DHS et les parties prenantes à la sécurité, autant du côté des propriétaires d'infrastructures que des opérateurs. Pour plus d'information, voir le site du Homeland Security : Regional Directors and Protective Security Advisor, http://www.dhs.gov/files/programs/gc_1265310793722.shtm

24 Le National Infrastructure Advisory Council (NIAC) est un comité consultatif responsable de conseiller le Président en formulant des avis sur la sécurité en matière de protection des infrastructures essentielles et leurs systèmes d'information.

25 Recherche et développement pour la défense du Canada. 2010. Protection des infrastructures essentielles (PIE), modifié 10 février. http://www.css.drdc-rddc.gc.ca/pstp/priorities-priorites/cip-pie-fra.asp

26 Cette stratégie de cybersécurité s'additionne aux mesures déjà en place à la GRC depuis plusieurs années. L'organisation a une division spéciale, appelé le Critical Infrastructure Criminal Intelligence (CICI), au sein d'un de ses programmes de sécurité nationale depuis plusieurs années (Thatcher, 2011).

27 Voir plus spécifiquement la page web *Sûreté des infrastructures stratégiques*, 2010.

28 Cette Direction se trouve sous la Direction générale des affaires policières qui conseille le ministre, notamment en matière de lutte contre le crime organisé et le terrorisme, ainsi que sur la sécurité publique et de l'État (Sécurité publique Québec, 2010, a, b).

29 EPCIP acronyme du titre anglais European Program for Critical Infrastructure Protection.

30 En 2005, le CIWIN est créé et réunit les spécialistes des États membres afin qu'ils soutiennent la Commission européenne dans l'élaboration de programmes visant à faciliter l'échange d'information sur les menaces et les vulnérabilités ainsi que sur les mesures et stratégies appropriées pour y faire face. EurActiv. 2006. Critical Infrastructure, 13 décembre. http://www.euractiv.com/en/security/critical-infrastructure/article-140597.

Bibliographie

Toutes les pages consultées en ligne ont été vérifiées et étaient actives à la date de publication de ce rapport.

Abele-Wigert, Isabelle and Myriam Dunn. 2006. "An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies", in *International CIIP Handbook* 2006, vol. 1, Center for Security Studies, ETH Zurich.www.crn.ethz.ch/publications/crn_team/detail.cfm?id=16651

Brunner, Elgin M. and Manuel Suter. 2008. *International CIIP Handbook 2008 / 2009 : An Inventory Of 25 National And 7 International Critical Information Infrastructure Protection Policies*, Center for Security Studies, ETH Zurich.

Burgess, J. Peter and Sissel Haugdal Jore. 2008. T*he Influence of Globalization on Societal Security: The Norwegian Context*, 4. http://www.prio.no/sptrans/-82857005/The%20Influence%20of%20Globalization%20on%20Societal%20Security%20-%20The%20Norwegian%20Context.pdf

Centre de politique de sécurité internationale (CPSI). 2004. *Swiss Update : Politique extérieure et protection des infrastructures critiques*, Septembre. http://www.eda.admin.ch/etc/medialib/downloads/edazen/topics/peasec/sec.Par.0036.File.tmp/SchutzKritischerInfrastrukturen_fr.pdf

Coursaget, Alain. « La sécurité des activités d'importance vitales: premier bilan du SGDSN », *Sécurité et Stratégie*, n° 4, novembre 2010 / mars 2011 : 5-17.

CRN - Crisis and Risk Network. 2009. *Critical infrastructure protection*, Focal Report 2, Center for Security Studies (CSS), ETH Zürich Commissioned by the Federal Office for Civil Protection (FOCP), Zurich, March.

CSS - Centre des sciences pour la sécurité. 2010. P*rotection des infrastructures essentielles : Résumé de la communauté de praticiens*, Recherche et développement pour la défense du Canada, Gouvernement du Canada. http://www.css.drdc-rddc.gc.ca/pstp/proj-prop/call-appel/infrastructure/infrastructure_s00-fra.pdf

Daguzan, Jean-François. 2010. « La protection des infrastructures critiques, l'enjeu stratégique du XXIe siècle », *AFRI – Annuaire français des relations internationales*, vol. XI :1001-1015.

Dunn Cavelty, Myriam. 2010. *Critical Infrastructure: From Protection to Resilience*, ISN-ETH Zurich, 17 February. http://www.isn.ethz.ch/isn/layout/set/print/content/view/full/73?id=123603&lng=en

Dunn Cavelty, Myriam. 2007. « Les infrastructures essentielles de l'information : failles, menaces et parades », Les technologies de l'information et la sécurité internationale – forum du désarmement, 3, 19-23.

Dunn, Myriam. 2007. « Critical Infrastructures: Vulnerabilities, Threats, Responses », CSS Analyses in *Security Policy*, vol. 2, n° 16, June : 1-3.

Environnement Canada. 2011. A*vertissements météo publics pour le Canada : Programme d'alertes à la population*, 13 avril. http://www.ec.gc.ca/meteo-weather/default.asp?lang=Fr&n=C9A8D735-1

EurActiv. 2006. *Critical Infrastructure*. 13 décembre. http://www.euractiv.com/en/security/critical-infrastructure/article-140597

Fildes, Jonathan. 2011. "Stuxnet virus targets and spread revealed", *BBC News*, 15 February. http://www.bbc.co.uk/news/mobile/technology-12465688

GAO – United States Government Accountability Office. 2010. *Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened*, Washington D.C. September.

Hammond, Brian. 2011. "Cybersecurity Among Top Priorities Of Homeland Security Consortium" *Cybersecurity Policy Report*, New York, January 10.

Hémond Yannick et Benoît Robert. 2010. « Evaluation of the Consequences of Road System Failure on Other Critical Infrastructures », *International Journal of Critical Infrastructures*, vol.6, n° 1 : 1-16.

Jopling, Lord. 2007. *162 cds 07 f rév 1 - La protection des infrastructures critiques*, Rapporteur special (Royaume-Uni). Rapports de commission, Assemblée parlementaire de l'OTAN. http://www.nato-pa.int/default.asp?CAT2=1159&CAT1=16&CAT0=2&COM=1165&MOD=0&SMD=0&SSMD=0&STA=&ID=0&PAR=0&LNG=1

Marie-Christine Therrien. 2010. « Stratégie de résilience et infrastructures essentielles », *Télescope*, vol. 16, n° 2, printemps-été : 154-171.

Miller, Robert A. 2009. « There's infrastructure and . . . critical infrastructure », I*nternational Journal of Critical Infrastructure Protection*, vol. 2 : 3-4.

Ministère des Relations internationales. 2006. *Politique internationale du Québec : La force de l'action concertée*, Gouvernement du Québec.

Moteff, John D. 2010. *Critical Infrastructures: Background, Policy, and Implementation*, Congressional Research Service, Report for Congress, June 7.

Neault, Jean-Marc. 2009. « Démarche de planification gouvernementale : la résilience des systèmes essentiels au Québec », *Résilience*, Bulletin d'information en sécurité civile du ministère de la Sécurité publique, vol. 4, n°1, hiver - printemps 2009 : 4-5. http://www.aqbrs.ca/Documents/SecuriteCivile/Resilience_vol4_no1_hiver_printemps_09.pdf

OCDE – Organisation de coopération et de développement économiques. 2008. « Les infrastructures à l'horizon 2030, volume 2 : Électricité, eau et transports : quelles politiques?) », *Synthèses*, Février.

RC - Radio-Canada. 2010. *Washington désigne les sites d'intérêt stratégique au Canada*, lundi 6 décembre. http://www.radio-canada.ca/nouvelles/International/2010/12/06/004-wikileaks-sites-strategiques-canadiens.shtml

RDDC - Recherche et développement pour la défense du Canada. 2010. *Protection des infrastructures essentielles* (PIE), modifié 10 février. http://www.css.drdc-rddc.gc.ca/pstp/priorities-priorites/cip-pie-fra.asp

Renda, Andrea and Bernard Hämmerli. 2010. *Protecting Critical Infrastructure in the EU*. CEPS - Centre for European Policy Studies Task Force Report, 16 December.

Robert, Benoît, Hémond, Yannick et Gabriel Yan. 2010. « L'évaluation de la résilience organisationnelle », *Télescope*, vol. 16, n° 2, printemps-été : 131-153.

Robert, Benoît et Luciano Morabito. 2008. « Les effets domino », *The CIP Exchange*, Spring, p. 7-9. http://spa.management.dal.ca/Files/CIP/CIP_Exchange_May_2008.pdf

Robert, Benoît, Wagner, Guillaume et Yannick Hémond. 2008. *Réflexions sur la place de l'humain dans les interdépendances entre infrastructures essentielles*, Centre Risque & Performance – document de travail. http://www.polymtl.ca/crp/doc/CRPDT2008_IEetressourcehumaine.pdf

Sécurité publique Canada. 2009. *Loi sur la gestion des urgences*, modifié 5 juin. http://www.publicsafety.gc.ca/media/nr/2007/bk20070807-fra.aspx

Sécurité publique Canada. 2009a. *Stratégie nationale sur les infrastructures essentielles*. http://www.publicsafety.gc.ca/prg/em/ci/_fl/ntnl-fra.pdf

Sécurité publique Canada. 2010. *Stratégie nationale sur les infrastructures essentielles*, 28 mai 2010. http://www.securitepublique.gc.ca/prg/em/ci/ntnl-fra.aspx http://www.securitepublique.gc.ca/prg/em/ci/_fl/ntnl-fra.pdf

Sécurité publique Canada. 2010a. *Plan d'action canado-américain sur les infrastructures essentielles*, modifié 16 juillet. http://www.securitepublique.gc.ca/prg/em/ci/cnus-ct-pln-bkgr-fra.aspx

Sécurité publique Canada. 2011. *Résumé quotidien de Sécurité publique Canada sur les infrastructures*. http://www.securitepublique.gc.ca/dir/index-fra.aspx

Sécurité publique Canada. 2011a. *DIR11-100 - 26 mai 2011 : Liens utiles*. http://www.securitepublique.gc.ca/dir/dir11-100-fra.aspx?rss=false

Sécurité publique Québec. 2009. *Centre de gestion de l'information de sécurité*, Gouvernement du Québec, mis à jour le 09 décembre, http://www.securitepublique.gouv.qc.ca/police/securite-etat/information-securite.html

Sécurité publique Québec. 2009a. *Démarche gouvernementale de résilience des systèmes essentiels*, mis à jour le 11 mars. http://www.securitepublique.gouv.qc.ca/securite-civile/securite-civile-quebec/activites-evenements/colloque/colloque-2009/1173.html

Sécurité publique Québec. 2010. *Sûreté des infrastructures stratégiques*, Gouvernement du Québec, mis à jour le 25 février. http://www.securitepublique.gouv.qc.ca/police/securite-etat/protection-infrastructures.html

Sécurité publique Québec. 2010a. *Direction générale des affaires policières*, Gouvernement du Québec, mis à jour le 24 septembre. http://www.securitepublique.gouv.qc.ca/ministere/structure/mandat-dgap.html

Sécurité publique Québec. 2010b. *Lutte contre le terrorisme*, Gouvernement du Québec, mis à jour le 5 mars. http://www.securitepublique.gouv.qc.ca/police/securite-etat/lutte-contre-terrorisme.html

Svedin, Lina. 2009. « Diverging and Converging Policy Paths: Critical Infrastructure Protection in the United States and the European Union » *Paper presented at the annual meeting of the ISA's 50th Annual Convention « Exploring The Past, Anticipating The Future »*, New York Marriott Marquis, New York City, USA, February 15, en ligne depuis le 8 février 2011. http://www.allacademic.com/meta/p311598_index.html

Thatcher, Chris. 2011. "Cyber strategy: Defining roles in a federated model", interview with Robert Dick, *Vanguard*, February - March : 10-11.

Thatcher, Chris. 2011a. "Critical Threats: Infrastructure protection in a new landscape", *Vanguard*, February - March : 12-14.

Weston, Greg. 2011. "Foreign hackers attack Canadian government Computer systems at 3 key departments penetrated", *CBC News*, Posted: Feb 16, 2011 8:59 PM ET - Last Updated: Feb 17, 2011. http://www.cbc.ca/news/technology/story/2011/02/16/pol-weston-hacking.html

Zetter, Kim. 2010. "WikiLeaks Releases Secret List of Critical Infrastructure Sites", *Threat Level: Privacy, Crime and Security Online*, December 6. http://www.wired.com/threatlevel/2010/12/critical-infrastructures-cable/

Le Laboratoire d'étude sur les politiques publiques et la mondialisation a été créé en 2004 par une entente de partenariat entre le ministère des Relations internationales et l'ENAP. Le Laboratoire est un lieu de veille et d'analyse consacré à l'étude des effets de la mondialisation sur le rôle de l'État et sur les politiques publiques au Québec, et ce sur les enjeux d'ordre culturel, économique, environnemental, de santé, d'éducation et de sécurité.

Relations internationales Québec

Directeur : Paul-André Comeau

Pour renseignements :
Karine Plamondon
Téléphone : (418) 641-3000 poste 6864
leppm@enap.ca

Les publications du Laboratoire peuvent être consultées sur le site :
www.leppm.enap.ca

Pour citer ce document :

TREMBLAY, Monica. Les infrastructures essentielles : un défi pour la sécurité des États. Québec, Laboratoire d'étude sur les politiques publiques et la mondialisation, ENAP, 2011, 21 p. (Rapport évolutif. Analyse des impacts de la mondialisation sur la sécurité au Québec; Rapport 10).

ENAP
L'Université de l'administration publique

Dépôt légal - Bibliothèque et Archives nationales du Québec, 2011
Dépôt légal - Bibliothèque et Archives Canada, 2011

ISBN978-2-923856-33-9 (version imprimée)
ISBN 978-2-923856-34-6 (PDF)