Concours Étudiant - RECO Québec 2015

1er Prix – M. Étienne Després

Afin d'encourager la relève en continuité et de favoriser les échanges d'idées, RECO Québec est fier de lancer son premier concours étudiant. Cette récompense vise à reconnaitre le travail de recherche étudiant qui se distingue dans le domaine de la continuité des opérations et de la gestion de crise.

Candidature

Identification du candidat	
Prénom Nom	Étienne Després
Adresse courriel	etienne.despres@usherbrooke.ca
Université	Université de Sherbrooke
Programme universitaire	Politiques publiques et relations internationales
Diplôme attendu	Maîtrise ès Arts
Présentation du parcours académique, professionnel, associatif *(max 200 mots)*	L'auteur a terminé son baccalauréat en Études est-asiatiques et Anthropologie en se spécialisant sur la Chine. Il a également passé six mois à l'Université de Lanzhou avant de continuer son parcours académique à l'École de politique appliquée de l'Université de Sherbrooke. M. Després a fait son stage au sein de la Direction Continuité des affaires chez Desjardins, où il a été engagé par la suite comme employé temporaire en tant qu'agent de soutien. Son contrat terminé, il se penche maintenant sur un contrat de recherche sur la coopération du Canada et des États-Unis en matière de protection et de résilience des infrastructures essentielles. Également, dans le cadre de l'écriture de son travail dirigé, il s'intéresse au contre-terrorisme chinois et au rôle de l'Organisation de coopération de Shanghai dans la lutte régionale au terrorisme.

Article

Titre
La continuité des opérations dans la protection des infrastructures essentielles : vers une approche régionale intégrée
Article *(max 1250 à 2000 mots)*

Introduction

Certaines entreprises au Québec et au Canada sont ce que l'on considère des infrastructures essentielles (IE)[1]. Au Québec, on entend par infrastructure essentielle « une infrastructure[2] 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[3]. » Au Québec, les différentes IE sont regroupées en dix catégories : l'énergie et les services publics, les technologies de l'information et des communications, les finances, la santé, l'alimentation, l'eau, les transports, la sécurité, le gouvernement, et, finalement, les industries[4].

Une stratégie et un plan d'action ont été établis au niveau national afin de protéger et de rendre résilient ces infrastructures[5]. La stratégie nationale repose sur trois piliers : (1) établir des partenariats; (2) mettre en œuvre une approche de gestion tous risques et; (3) favoriser l'échange en temps opportun entre les partenaires et la protection de cette information[6]. Également, une approche conjointe a été développée entre le Canada et les États-Unis dans le cadre du Plan d'action par-delà la frontière[7].

Constatant l'importance que devrait avoir la continuité des affaires dans la résilience des IE, mais que bien peu d'efforts sont faits par le gouvernement fédéral pour inciter une gestion efficace de la continuité, une approche régionale de la gestion de la continuité des affaires sera mise de l'avant dans ce texte. C'est une approche qui se développe rapidement et qui fait ses preuves. D'abord, nous constaterons que la continuité des opérations serait un outil efficace dans la résilience des IE, mais qu'elle n'est pas assez mise de l'avant par le gouvernement fédéral. Ensuite, nous définirons les attributs d'une approche régionale dans la résilience des infrastructures essentielles et les bienfaits d'une telle approche pour les gestionnaires en continuité des affaires.

Des infrastructures résilientes

La résilience est au cœur de la stratégie gouvernementale, et en explorant ce concept, il est évident que la continuité des affaires est un outil particulièrement pertinent. En effet, la résilience fait référence à la capacité d'un système[8] à se rétablir d'un événement dommageable et qui aurait pu avoir des conséquences catastrophiques[9]. Par exemple, alors qu'un système axé sur la protection aurait engagé des gardiens de sécurité pour éviter certaines catastrophes, une organisation résiliente organiserait un site de relève où les activités critiques peuvent être reprises dans un court délai. Évidemment, la protection et la résilience ne sont pas deux domaines mutuellement exclusifs, mais la différence de philosophie est importante. En mettant l'emphase sur la résilience, une organisation accepte qu'elle n'est pas à l'abri de disruptions importantes, alors que la protection tente d'éviter toute disruption.

L'objectif de la gestion de la continuité, selon le DRI, est « de rendre l'entité plus résiliente aux menaces possibles et de lui permettre de reprendre ou de continuer d'opérer dans des conditions défavorables ou anormales[10] ». La continuité

des activités est ainsi un outil essentiel pour toute entreprise qui vise à devenir résiliente bien que d'autres disciplines managériales travaillent également en ce sens[11].

Malgré le lien évident entre la résilience des IE et la continuité des activités, le gouvernement a fait très peu d'efforts pour s'assurer que les entreprises privées considérées comme essentielles aient un plan de continuité des opérations qui soit fonctionnel et exercé. Ce travail est plutôt relégué, dans certains cas, à des organismes de réglementation qui émettent des lignes directrices en matière de gestion des risques et de continuité des affaires. Par exemple, l'Autorité des marchés financiers, au Québec, a publié une ligne directrice en matière de continuité des activités qui vise les institutions financières[12]. Seulement, dans la plupart des cas, les organismes de réglementation gouvernementaux demandent plutôt aux entreprises une assurance de service[13]. La façon dont le niveau de service est assuré est souvent à la discrétion de l'organisation et c'est seulement l'audit interne qui permet de vérifier la crédibilité d'un programme de continuité des affaires. Clairement, un programme gouvernemental d'incitatifs financiers visant à encourager les propriétaires privés et publics des IE à mettre en place et exercer leur plan de continuité serait bénéfique.

Les forums sectoriels et le forum inter-sectoriel mis en place à travers la stratégie nationale ont le potentiel d'être un endroit où les acteurs pertinents peuvent échanger sur ce sujet, mais l'efficacité de ces forums a été remise en question en 2012 par le vérificateur général du Canada[14]. Une approche nationale semble donner peu de résultats. Il appert qu'une approche régionale serait une alternative efficace et qui s'harmoniserait bien avec les efforts binationaux actuels des gouvernements d'Ottawa et de Washington dans le cadre du plan d'action *Par-delà la frontière*. Celui-ci mets de l'avant une approche régionale dans la protection et la résilience des IE.[15] Dans le cadre de ce plan d'action, une analyse régionale des vulnérabilités du Maine et du Nouveau-Brunswick a déjà été élaborée. Depuis 2014, c'est la région qui inclut la Colombie-Britannique, l'Alaska et le Yukon qui est sous la loupe[16].

Développer une perspective régionale

La gestion de la continuité des opérations au sein des entreprises qui font partie de l'un des secteurs des IE au Canada et au Québec doit être réévaluée. En effet, la gestion de la continuité des opérations se concentre sur l'entreprise comme le noyau qui doit être protégé. Cela semble évident, surtout en considérant que c'est effectivement l'entreprise qui assume les coûts liés à la continuité des affaires. Seulement, toute entreprise est influencée par son environnement, et, à son tour, l'influence. Les entreprises ne sont pas comme des entités indépendantes, mais sont bel et bien des rouages dans un système complexe, dont toutes les parties sont interdépendantes. Les conséquences d'une défaillance d'une IE peuvent être désastreuses pour la communauté et pour d'autres IE. Nous n'avons qu'à penser aux événements de la tempête de verglas en 1998 et à la panne d'électricité au sud de l'Ontario et dans le nord-est des États-Unis en 2003 pour constater les effets néfastes d'une défaillance régionale.

Étant donné la nature du système dans lequel nos sociétés évoluent, il apparaît que les gestionnaires en continuité des affaires ne peuvent plus seulement prendre en compte leur entreprise dans l'évaluation des vulnérabilités et dans l'élaboration des plans de continuité des affaires. Cette idée est de plus en plus répandue au sein du domaine de la continuité, comme le démontre l'intérêt envers une nouvelle conséquence qui représente les chaînes d'approvisionnement : la perte d'un fournisseur essentiel. Toutefois, la façon dont est prise en compte cette vision plus englobante et holiste devrait être plus ambitieuse si l'on veut évoluer dans un système réellement résilient.

Les propriétaires et les gestionnaires de la continuité des affaires d'IE doivent décloisonner leur gestion de la continuité de l'entreprise à une perspective régionale. Ces régions ne devraient pas être qualifiées en fonction des frontières géographiques, mais des nexus naturels au sein de la société, c'est-à-dire les chaînes d'approvisionnement, la mobilité fréquente au sein d'un endroit donné, l'intégration économique, etc. Même la frontière entre le Canada et les États-Unis ne devrait pas être considérée dans l'identification d'une région donnée : l'importance économique de la frontière démontre en effet qu'il faut être inclusif plutôt qu'exclusif. Considérer qu'une région se termine à la frontière ne tient

pas compte de l'importance de celle-ci pour la population et les entreprises à proximité de celle-ci. La protection de la frontière doit se faire avec des méthodes traditionnelles déjà mises en place, mais la résilience régionale des IE implique que les acteurs des deux côtés de la frontière doivent travailler ensembles. Également, toute organisation régionale doit inclure les parties prenantes publics et privés.

Le meilleur exemple de ce type d'organisation est la *Pacific Northwest Economic Region* (PNWER)[17]. Elle inclut des provinces de l'ouest canadien ainsi que des États du nord-ouest des États-Unis et est composée de représentants du milieu public, du milieu privé et d'organisations non-gouvernementales. La PNWER a créé en 2001 le *Center for Regional Disaster Resilience* (CRDR)[18]. Le CRDR constate que « les économies interconnectées de notre région et nos infrastructures essentielles partagées sont sujets à des désastres aux impacts en cascades et d'une portée considérable. »[19] Les champs d'intérêt du CRDR incluent la résilience des chaînes d'approvisionnement, la cybersécurité, les interdépendances, le partage de l'information et le rétablissement suite à un désastre. Plusieurs initiatives régionales ont lieu avec les parties prenantes du CRDR : des exercices de gestion de crise régionales se tiennent régulièrement, des séminaires sont organisés, des plans sont élaborés, au point où la priorisation régionale de l'accès à la nourriture, à l'eau et au pétrole est l'une des prochaines étapes[20]. Le CRDR est définitivement un modèle à suivre pour la résilience régionale.

Les gestionnaires de continuité des affaires auraient plusieurs avantages à participer à une organisation régionale telle que le CRDR : une meilleure compréhension des interdépendances régionales, un partage sur les meilleures pratiques, un contact direct avec les autres intervenants publics et privés, une facilité d'accès à des informations en cas de crise, la possibilité d'organiser des exercices régionaux, etc. Pour y arriver, les gestionnaires en continuité des affaires doivent considérer leur organisation comme faisant partie d'un système plutôt que de considérer leur organisation comme un système en soi, qui n'est pas affecté par son environnement.

Conclusion

Développer une approche régionale de la résilience dans laquelle la continuité des activités serait un aspect incontournable demandera une volonté et une mobilisation autant de la part du gouvernement que des propriétaires d'infrastructures essentielles. Les initiatives gouvernementales démontrent que la volonté politique existe, mais des incitatifs doivent être développés. Il est grand temps que les gestionnaires en continuité des activités considèrent leur organisation en fonction des réalités régionales et participent initiatives et aux partenariats dans la résilience des IE. La résilience organisationnelle n'en sera que plus solide, la gestion en situation de crise plus efficace et le rétablissement post-désastre plus rapide. Il est grand temps que les pratiques en continuité des affaires reflètent la réalité des interdépendances régionales des IE.

Bibliographie

Documents officiels

GOUVERNEMENT DU CANADA. (2004). *Protéger une société ouverte : la politique canadienne de sécurité nationale*, 59 pages.

GOUVERNEMENT DU CANADA. (2009). *Stratégie nationale sur les infrastructures essentielles*, Sécurité publique Canada, 10 pages.

HOMELAND SECURITY ET SÉCURITÉ PUBLIQUE CANADA. (2010). *Canada-United States Action Plan for Critical Infrastructure*, 9 pages.

CONFERENCE BOARD OF CANADA. (2011). *Regional, Cross-Border Planning: Maine – New Brunswick Action Plan for*

Infrastructure Protection and Resilience, National Security and Public Safety, 58 pages.

GOUVERNEMENT DU CANADA. (2011). *Plan d'action de résilience aux incidents chimiques, biologiques, radiologiques, nucléaires et à l'explosif pour le Canada*, Sécurité Publique Canada, 10 pages.

GOUVERNEMENT DU CANADA. (2011). *Plan d'action par-delà la frontière : une vision commune de la sécurité du périmètre et de la compétitivité économique*, Sécurité Publique Canada, 42 pages.

GOUVERNEMENT DU CANADA. (2012). *Plan d'action sur la cybersécurité entre Sécurité publique Canada et le Département de la Sécurité intérieure*, Sécurité publique Canada, 4 pages.

GOUVERNEMENT DU CANADA. (2012). *Plan nord-américain contre l'influenza animale et la pandémie d'influenza*, Sécurité publique Canada, 84 pages.

GOUVERNEMENT DU CANADA. (2012). *Chapitre 3 : Protéger l'infrastructure canadienne essentielle contre les cybermenaces*, tiré du *Rapport du vérificateur général à la Chambre des communes*, Bureau du vérificateur général, 34 pages.

GOUVERNEMENT DU CANADA. (2013). *Canada-United States Beyond the Border Action Plan Implementation Report*, Sécurité publique Canada, 12 pages.

GOUVERNEMENT DU CANADA. (2014). *Plan d'action sur les infrastructures essentielles 2014-2017*, Sécurité publique Canada, 16 pages.

GOUVERNEMENT DU CANADA. (2015). *Bulletin Plan d'action par-delà la frontière été 2015*, Sécurité publique Canada, 5 pages.

GOUVERNEMENT DU CANADA. (2015). *Canada – États-Unis Plan d'action par-delà la frontière : Rapport sur la mise en œuvre mars 2015*, Sécurité publique Canada, 26 pages.

GOUVERNEMENT DU CANADA. (2009). *Plan d'action sur les infrastructures essentielles*, Sécurité publique Canada, 25 pages.

Articles scientifiques

ANSELL, Chris *et al.* (2010). « Managing Transboundary Crises : Identifying the Building Blocks of an Effective Response System », *Journal of Contingencies and Crisis Management*, 18:4, pp. 195-207.

AUERSWALD, Philip *et al.* (2005). « The Challenge of Protecting Critical Infrastructure », *Issues in Science and Technology*, 22:1, pp. 77-83.

BOIN, Arjen et MCCONNELL, Allan. (2007). « Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience », *Journal of Contingencies and Crisis Management*, pp. 50-59.

BOW, Brian. (2014). « Now for the Hard Part : Renewing Regional Cooperation on Critical Infrastructure Security and Resilience », *Wilson Center et le Conseil international du Canada*, 18 pages.

COMFORT, Louise K. (2002). « Rethinking Security: Organizational Fragility in Extreme Events », *Public Administration Review*, 62, pp. 98-107.

CHRISTOPHERSON, Susan *et al.* (2010). « Regional resilience : theoretical and empirical perspectives », *Cambridge Journal of Regions, Economy and Society*, 3, pp. 3-10.

DE BRUIJNE, Mark et VAN EETEN, Michel. (2007). « Sytems that Should Have Failed: Critical Infrastructure Protection in

an Institutionally Fragmented Environment », *Journal of Contingencies and Crisis Management*, 15:1, pp. 18-29.

DE LAAT, William. (2012). « The Beyond the Border Action Plan : A Tool for Enhanced Canada-U.S. Cooperation on Critical Infrastructure and Cyber Security – Or More Window Dressing? » *Canada-United States Law Journal*, 37:2, pp. 451-468.

GRAHAM, Andrew. (2011). « Canada's Critical Infrastructure : When is Safe Enough Safe Enough? », *The Macdonald-Laurier Institute*, 32 pages.

GRASHOFF, Matthew K. (2012). « Building Fences Together : The EU's Lessons for the U.S.-Canada Perimeter Security Plan », *Canada-United States Law Journal*, 37:2, pp. 517-550.

MCDANIEL, Michael C. (2012). « Beyond 'Beyond the Border' : A Proposal for Implementation of the Action Plan's Recommendation on Cross-Border Critical Infrastructure », *Canada-United States Law Journal*, 37:2, pp. 433-449.

QUIGLEY, Kevin. (2013). « Man plans, God laughs : Canada's national stratefy for protecting critical infrastructure », *Canadian public administration / Administration publique du Canada*, 56:1, pp. 142-164.

RINALDI, S.M. *et al.* « Identifying, understanding, and analyzing critical infrastructure interdependencies », *Control Systems, IEEE*, 21:6, pp. 11-25.

Thèses et mémoires

LAWRENCE CARPENTIER, Michel. (2007). « Canada and 9/11 : Border Security in a New Era », Mémoire soumis au Département d'études politiques en vue de l'obtention d'une maîtrise, Université de Saskatchewan, 104 pages.

Sites web

CENTER FOR REGIONAL DISASTER RESILENCE. (s.d.). *Center for Regional Disaster Resilience – Home*, [En Ligne], Pacific NorthWest Economic Region, http://www.regionalresilience.org/

GOUVERNEMENT DU CANADA. (2014). *Cybersécurité et protection de l'indfrastructure essentielle*, [En Ligne], Service canadien du renseignement de sécurité, https://www.csis-scrs.gc.ca/ththrtnvrnmnt/nfrmtn/index-fr.php

GOUVERNEMENT DU CANADA. (2014). *Infrastructures essentielles*, [En Ligne], *Sécurité publique Canada*, http://www.securitepublique.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-fra.aspx

GOUVERNEMENT DU QUÉBEC. (2010). *Sûreté des infrastructures stratégiques*, [En Ligne], Sécurité publique Québec, http://www.securitepublique.gouv.qc.ca/police/securite-etat/protection-infrastructures.html

[1] Le gouvernement du Québec utilise également le terme « infrastructure stratégique », mais réfère au même concept.
[2] Une infrastructure peut être une installation, un système, un réseau ou un encore un bien.
[3] Gouvernement du Québec. (2010). *Sûreté des infrastructures stratégiques*, Sécurité Publique Québec, [En Ligne], http://www.securitepublique.gouv.qc.ca/police/securite-etat/protection-infrastructures.html (page consultée le 27 octobre 2015).
[4] *Ibid.*
[5] Voir à ce sujet Gouvernement du Canada. (2009). *Stratégie nationale sur les infrastructures essentielles*, Sécurité publique Canada et Gouvernement du Canada. (2009). *Plan d'action sur les infrastructures essentielles*, Sécurité publique Canada.
[6] *Ibid.*
[7] Voir à ce sujet Gouvernement du Canada. (2011). *Plan d'action par-delà la frontière : une vision commune de la sécurité du périmètre et de la compétitivité économique*, pp. 29-34.
[8] Un système peut être à différents niveaux : une entreprise, une industrie, une région, une société, une nation, etc.
[9] Dunn Cavelty, M. (2010). *Critical infrastructure: From protection to resilience*, ISN ETH Zurich, [En Ligne], http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?lng=en&id=123603 (page consultee le 29 octobre 2015).
[10] DRI International. (2012). *Les pratiques professionnelles pour professionnels en continuité d'activités*, p.1.
[11] Business Continuity Institute. (2013). *…Guide de mise en œuvre des bonnes pratiques de continuité d'activité,* p.12.
[12] Voit Autorité des marchés financiers. (2010). *Ligne directrice sur la gestion de la continuité des activités*, [En Ligne], https://www.lautorite.qc.ca/files/pdf/reglementation/lignes-directrices-toutes-institutions/2010mars31-ld-gestion-continuite-fr.pdf
[13] Par exemple, le CRTC fonctionne de cette façon dans le domaine des télécommunications.
[14] Gouvernement du Canada. (2013). *Déclaration d'ouverture au Comité permanent des comptes publics : Protéger l'infrastructure canadienne essentielle contre les cybermenaces*, Bureau du vérificateur général du Canada, [En Ligne], http://www.oag-bvg.gc.ca/internet/Francais/osh_20130423_f_38313.html (page consultée le 29 octobre 2015).
[15] Voir Gouvernement du Canada. (2011). *Plan d'action par-delà la frontière : une vision commune de la sécurité du périmètre et de la compétitivité économique*, [En Ligne], http://plandaction.gc.ca/fr/page/bbg-tpf/dela-la-frontiere-plan-daction (page consultée le 3 novembre 2015).
[16] Voir à ce sujet Gouvernement Du Canada, *Plan d'action par-delà la frontière, op. cit.*, Gouvernement du Canada. (2013). *Beyond the Border Implementation Report – December 2013*, [En Ligne], http://www.actionplan.gc.ca/en/page/bbg-tpf/beyond-border-implementation-report-december-2013 (page consultée le 3 novembre 2015) et Gouvernement du Canada. (2015). *Rapport sur la mise en œuvre de l'initiative Par-delà la frontière – Mars 2015*, [En Ligne], http://plandaction.gc.ca/fr/contenu/rapport-mise-oeuvre-mars-2015 (page consultée le 3 novembre 2015).
[17] Voir leur site web : http://www.pnwer.org/
[18] Voir le http://www.regionalresilience.org
[19] Center for Disaster Resilience. (s.d.). *About us*, [En Ligne], http://www.regionalresilience.org/about-us.html (page consultée le 3 novembre 2015).
[20] Voir à ce sujet Center for Regional Disaster Resilience. (s.d.). *Critical Infrastructure Regional Integrated Action Strategy*, [En Ligne], http://www.regionalresilience.org/uploads/2/3/2/9/23295822/puget_sound_critical_infrastructure_regional_integrated_action_strategy.pdf (page consultée le 3 novembre 2015).