MLI

SOLUTIONS TO CRITICAL INFRASTRUCTURE PROBLEMS

Essays on Protecting Canada's Infrastructure

Jason Clemens and Brian Lee Crowley, Editors

3 NATIONAL SECURITY STRATEGY FOR CANADA SERIES

The Macdonald-Laurier Institute

"True North in Canadian Public Policy"

Board of Directors

Advisory Council

Research Advisory Board

The Macdonald-Laurier Institute exists to:

- **Initiate** and conduct research identifying current and emerging economic and public policy issues facing Canadians, including, but not limited to, research into defence and security, foreign policy, immigration, economic and fiscal policy, Canada-US relations, regulatory, regional development, social policy and Aboriginal affairs;
- **Investigate** and analyse the full range of options for public and private sector responses to the issues identified and to act as a catalyst for informed debate on those options;
- **Communicate** the conclusions of its research to a national audience in a clear, non-partisan way;
- **Sponsor** or organize conferences, meetings, seminars, lectures, training programs and publications using all media of communication (including, without restriction, the electronic media), for the purposes of achieving these objects;
- **Provide** research services on public policy issues, or other facilities, for institutions, corporations, agencies and individuals, including departments and agencies of Canadian governments at the federal, provincial, regional and municipal levels, on such terms as may be mutually agreed, provided that the research is in furtherance of these objects

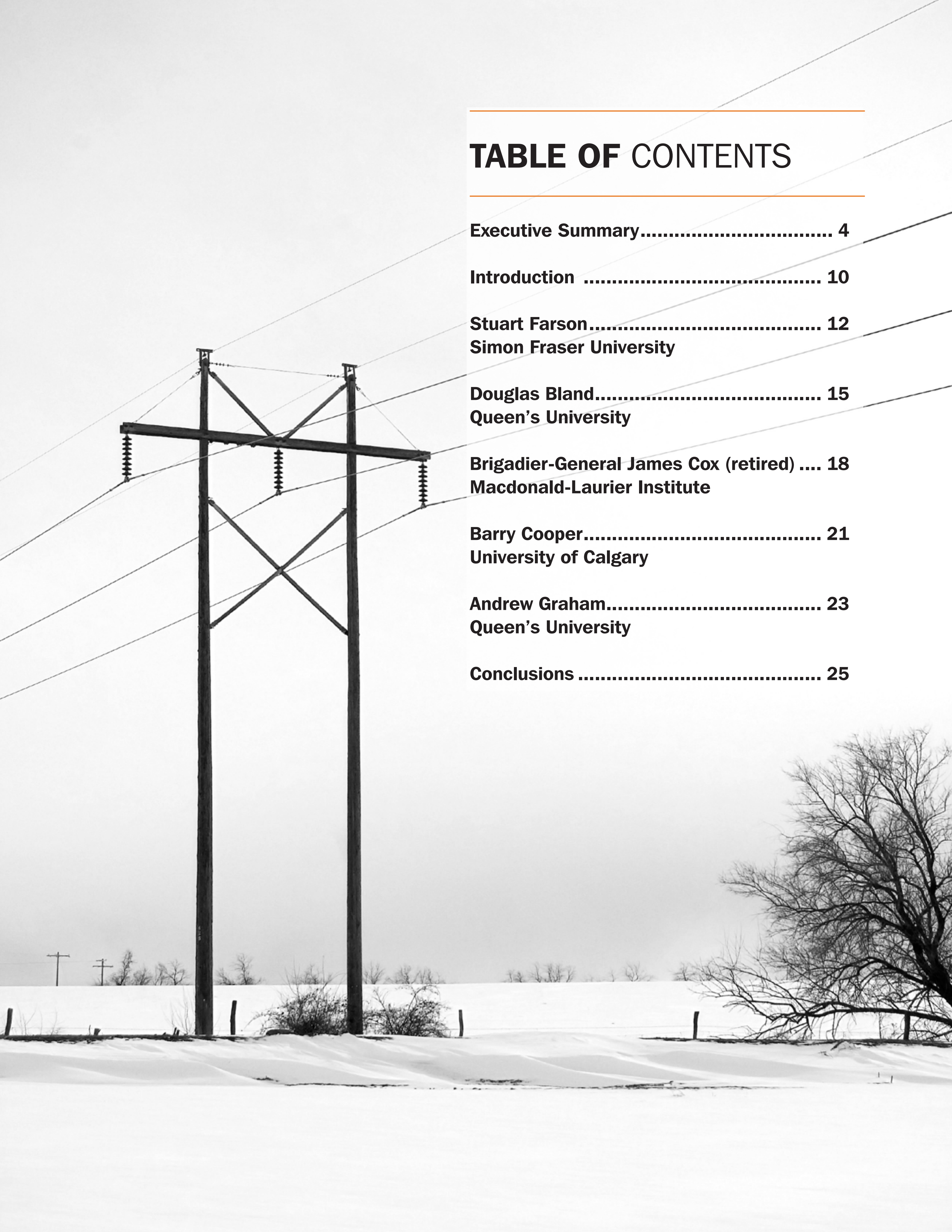

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Canada's critical infrastructure – the physical and cybernetic elements on which we rely to operate most modern services and systems – may be facing excessively high levels of risk from both natural disasters and human error or malice. The dispersed nature of this infrastructure heightens our vulnerability.

Dealing with this unique threat in advance requires that we understand its nature, and, once the real risks are identified, that we implement a cohesive, sustainable approach led by the federal government. Because the problem includes so many stakeholders, the federal government needs at the very least to develop a culture that increases the level of information shared among them and encourages communities of practice to mitigate potential disasters.

The federal government needs to develop a culture that encourages communities of practice to mitigate potential disasters.

In December, 2011, The Macdonald-Laurier Institute published a description of the problem, a study by Andrew Graham, Queen's University.[1] This paper contains essays from five scholars, including one from Graham, who discuss the vulnerability of Canada's critical infrastructure from their own perspectives, and who offer their thoughts on the means that the federal government might employ to reduce the country's exposure to harm.

Stuart Farson, from Simon Fraser University, warns against a "one size fits all" approach by Ottawa, and recommends embedding resiliency, rather than protection against all risk, as the primary value.

He argues that an adequate response to CI security threats or attacks is beyond the means of multiple local stakeholders. The federal government therefore needs to fund and co-ordinate protection strategies, and to collect and disseminate information about threats and risks. This would allow an "over the horizon" perspective, with feedback loops to determine what localized CI providers need.

Farson calls for a new, bifurcated federal agency. One part should be charged with assisting local agencies when required, with "How can we help?"as its mantra. It would offer a clearing-house for the collection, analysis and dissemination of information among government departments and infrastructure owners. The other part should focus on federal security, co-operation with other countries and threats that span provincial boundaries.

Douglas Bland, also from Queen's University, indicts the federal government's current approach as an incoherent "non-policy," a hodgepodge without even terms and definitions to guide it. He calls for a comprehensive solution re-invented from scratch. To counter objections that the federal government lacks the authority to do that, Bland points to its ability to intervene in other complicated policy files.

Bland wants changes based on 'vulnerability analysis' rather than 'risk analysis'. The first step is an inter-governmental agreement that defines criticality, security, domains of responsibility, funding criteria and needed regulatory instruments, followed by the construction of a new detailed regime of principles and processes to codify risks, and an inter-governmental convention to establish the regime.

As an example, the federal government would direct its own departments to develop CI security according to standards that describe degrees of criticality. Bland also calls for an inventory of CI systems, and an assessment of the value of each and the costs of repairing them. He reminds us that the primary aim of CI security is to ensure the continued delivery of essential goods and services to governments and Canadians.

"Vulnerability-based" rather than "risk-based" analysis.

James Cox, a retired Brigadier General in the Canadian Forces and a senior fellow of the Macdonald-Laurier Institute, is as critical as Bland of current federal policy. He cites palpable discontent in the CI community with a perceived reluctance to share information and intelligence. Cox says that local CI providers already co-operate among themselves, but need national direction.

Currently, working-level CI "operators" are not adequately consulted; they provide lists of infrastructure to the federal government, but the criticality of each is never assessed. Ottawa never mentions national standards or enforcement, but merely plans to pick up the pieces after debilitating events. Cox feels we should do more to engage the private sector with a formal structure for sectoral consultation, including training and emergency exercises, and a formal network for sharing information and intelligence, one with a two-way flow.

Barry Cooper is less pessimistic about the threat faced by Canada's critical infrastructure and less optimistic about the federal government's ability to deal with it.

The University of Calgary's Barry Cooper is less pessimistic about the threat faced by Canada's critical infrastructure and less optimistic about the federal government's ability to deal with it. The greatest real threats, he says, are natural disasters, not latent, manmade ones. Cooper notes that computerized systems also face "meta-threats" that must be assessed in terms of credibility, probability, and the severity of damage potential, and that measurement of that risk is always a matter of trade-offs.

Cooper says that Ottawa has both limited jurisdiction over security and a limited capacity to assure it. Zero risk is impossible, and resiliency of systems should define vulnerability. That limits the utility of central planning as a tool to reduce risk. He cautions against establishing a "bureaucratic nightmare," in which we do little but plan to plan, an effort necessarily peripheral to the delivery of real security.

Because CI is dispersed, Cooper points out, responsibility for its protection must be as well. Existing links between stakeholders and local police override the value of central co-ordination by Public Safety Canada, a fantasy. In Cooper's view, the most effective role for the federal government would be to restore the RCMP Commercial Crime Unit to an elite position in fighting cyber crime and meeting cyber threats.

Andrew Graham's recommendations for reform are set out in the last essay. They start with a call for new, more realistic system for assessing active risk, unlike the federal government's current focus on high-level, low-probability risk. He wants Ottawa to expand its processes to separate inherent risks from real ones, and to move it out of its closed loop by means of identification sessions that provide digestible chunks of information regularly updated.

Graham believes that the federal government's normal style of command and control systems is inadequate for the sharing of information and common approaches. He would prefer that

Ottawa engage actual CI operators, not just their organizations, in that task. Graham wants to expand local police involvement, and to integrate CI reporting into existing police intelligence systems.

Graham would prefer to see enhancements of infrastructure security delivered in the same way, through local police departments. But he wants the federal government to play an expanded role by establishing a CI Sector Council to foster research and training, by funding non-governmental centres of excellence to build knowledge and capacity, and by developing and testing case studies and risk scenarios in the real world. He encourages the use of tax incentives to promote the protection of critical infrastructure.

These five essayists share the view that the federal government needs fundamental changes in its approach to CI security. But the agreement ends there.

Farson, Bland, and Cox all seek formal, expanded activity by Ottawa in the field, and their recommendations range from the formal establishment of a new agency, to national conferences and conventions to set up a new federal process, to a less precise call for more national leadership. The solutions offered by both Cooper and Graham place more emphasis on the grassroots, with dispersed responsibility for monitoring and protecting CI in police departments, and, in Graham's case, in universities and a CI Council.

Five essayists share the view that the federal government needs fundamental changes in its approach to CI security.

SOMMAIRE

Les infrastructures essentielles (IE) du Canada – c'est-à-dire les éléments physiques et cybernétiques dont nous dépendons pour opérer la plupart des services et des systèmes modernes – pourraient être confrontées à des niveaux excessivement élevés de risque en provenance de désastres naturels et d'erreur ou de malveillance humaines. La nature dispersée de ces infrastructures accroît notre vulnérabilité.

Pour s'attaquer d'avance à cette menace particulière, il est nécessaire d'en comprendre la nature et, lorsque les risques réels auront été identifiés, de mettre en œuvre une approche cohésive et durable menée par le gouvernement fédéral. Parce que ce problème implique un grand nombre d'acteurs, le gouvernement fédéral doit au minimum développer une culture pour accroître la quantité de renseignements qu'ils se transmettent et pour encourager les communautés de pratique à atténuer les désastres potentiels.

En décembre 2011, l'Institut Macdonald-Laurier a publié une étude d'Andrew Graham de l'Université Queen's qui décrivait le problème . Le présent document contient des textes rédigés par cinq chercheurs, incluant un texte signé par M. Graham, qui discutent de la vulnérabilité des infrastructures essentielles canadiennes de leur point de vue. Chacun présente ses réflexions sur les moyens que le gouvernement fédéral pourrait prendre pour réduire l'exposition du pays à ces risques de dommages.

Le gouvernement fédéral doit développer une culture pour encourager les communautés de pratique à atténuer les désastres potentiels.

Stuart Farson de l'Université Simon Fraser nous met en garde contre une approche uniforme de la part d'Ottawa et recommande d'adopter comme valeur fondamentale un renforcement de la capacité du système à résister aux attaques, plutôt qu'une protection contre tous les risques.

Il soutient qu'une réponse adéquate aux menaces à la sécurité ou aux attaques contre les IE dépasse les capacités des nombreux acteurs locaux. Le gouvernement fédéral doit donc financer et coordonner les stratégies de protection, ainsi que recueillir et disséminer l'information reliée aux menaces et aux risques. Cela permettrait d'élaborer une perspective « au-delà de l'horizon » comportant des boucles de rétroaction pour déterminer ce dont les fournisseurs locaux d'IE ont besoin.

M. Farson en appelle à la création d'une nouvelle agence fédérale avec un double mandat. Une partie s'occuperait d'assister les agences locales lorsque le besoin s'en fait sentir, avec comme approche la question « Comment pouvons-nous vous aider? ». Elle servirait de centre de triage pour la collecte, l'analyse et la dissémination d'information au sein des ministères et parmi les propriétaires d'infrastructures. L'autre partie de l'agence se concentrerait sur la sécurité fédérale, la coopération avec d'autres pays et les menaces qui dépassent les frontières provinciales.

Douglas Bland, également de l'Université Queen's, dénonce l'approche actuelle du gouvernement fédéral qu'il qualifie de « non-politique » incohérente, un fouillis sans aucune condition ni définition pour le guider. Il demande la mise en place d'une solution exhaustive reconstruite de bout en bout. Pour répliquer à ceux qui disent que le gouvernement fédéral n'a pas l'autorité pour faire cela, M. Bland note que le gouvernement a été capable d'intervenir dans d'autres dossiers compliqués.

M. Bland souhaite que ces changements s'appuient sur une analyse fondée sur le « risque » plutôt que la « vulnérabilité ». La première étape consisterait en une entente intergouvernementale pour définir la criticité, la sécurité, les domaines de responsabilité, les critères de financement et les instruments réglementaires nécessaires. Cela serait suivi par l'élaboration d'un nouveau régime de principes et de processus détaillé pour codifier les risques, ainsi que par une convention intergouvernementale pour établir le régime.

Par exemple, le gouvernement fédéral demanderait à ses propres ministères d'assurer la sécurité des IE selon des normes décrivant les degrés de criticité. M. Bland propose également de mettre sur pied un inventaire des systèmes d'IE ainsi qu'une évaluation de la valeur de chacun et des coûts requis pour les réparer. Il nous rappelle que l'objectif premier de la sécurité des IE est d'assurer la livraison continue de biens et services essentiels aux gouvernements et à tous les Canadiens.

Une analyse fondée sur le « risque » plutôt que la « vulnérabilité ».

James Cox, un brigadier général des Forces armées canadiennes à la retraite et senior fellow à l'Institut Macdonald-Laurier, est tout aussi critique que M. Bland à l'égard de l'actuelle politique fédérale. Il note le mécontentement palpable au sein de la communauté des IE découlant de la réticence à partager l'information. M. Cox affirme que les fournisseurs locaux d'IE coopèrent déjà entre eux, mais qu'ils ont besoin d'un leadership national.

En ce moment, les « opérateurs » d'IE sur le terrain ne sont pas adéquatement consultés; ils fournissent des listes d'infrastructures au gouvernement fédéral, mais la criticité de chacune n'est jamais évaluée. Ottawa ne mentionne jamais les normes nationales d'exécution et se contente de se préparer à ramasser les pots cassés à la suite d'un événement qui provoquerait des dommages. M. Cox considère que nous devrions faire davantage pour impliquer le secteur privé dans le cadre d'une structure formelle de consultation sectorielle, y compris une formation et des exercices de préparation en cas d'urgence, de même qu'un réseau formel pour partager l'information dans les deux sens.

Le professeur Barry Cooper de l'Université de Calgary est moins pessimiste en ce qui a trait aux menaces envers les infrastructures essentielles du Canada et moins optimiste pour ce qui est de la capacité du gouvernement fédéral de s'y préparer. Selon lui, les plus importantes menaces concrètes sont les désastres naturels, et non des menaces cachées d'origine humaine. M. Cooper note que les systèmes informatiques sont également confrontés à des « méga menaces » qui doivent être évaluées sur le plan de leur crédibilité, de leur probabilité et de la sévérité des dommages potentiels. La mesure de ce risque est toujours une question d'arbitrage.

Barry Cooper de l'Université de Calgary est moins pessimiste en ce qui a trait aux menaces envers les infrastructures essentielles du Canada et moins optimiste pour ce qui est de la capacité du gouvernement fédéral de s'y préparer.

M. Cooper affirme qu'Ottawa possède à la fois des pouvoirs limités en ce qui a trait à la sécurité et une capacité limité de la garantir. Un risque nul est impossible et la résilience des systèmes devrait permettre de définir leur vulnérabilité. Cela limite l'utilité de la planification centralisée comme outil pour réduire le risque. Il nous met en garde contre la mise en place d'un « cauchemar bureaucratique », où l'on ne ferait que se préparer à planifier, un tel effort étant nécessairement secondaire par rapport à la fourniture d'une véritable sécurité.

M. Cooper note que comme les IE sont dispersées, la responsabilité pour leur protection doit l'être tout autant. Les liens existants entre les acteurs et la police locale l'emportent sur l'importance d'une coordination par Sécurité publique Canada, qui est un fantasme. De son point de vue, le rôle le plus efficace pour le gouvernement fédéral serait de redonner une position d'élite à la Sous-direction des délits commerciaux de la Gendarmerie royale du Canada pour lutter contre la cybercriminalité et les menaces informatiques.

Les recommandations d'Andrew Graham pour mettre en place des réformes sont présentées dans le dernier texte. Elles débutent par un appel à instaurer un nouveau système plus réaliste pour évaluer le risque actif, par opposition à la préoccupation actuelle du gouvernement fédéral envers le risque de haut niveau et de probabilité peu élevée. Il souhaite que le gouvernement fédéral élargisse ses processus de façon à séparer les risques inhérents des risques réels, et qu'il les extrait de sa boucle fermée au moyen de sessions d'identification qui fourniront des morceaux d'information digestibles régulièrement mis à jour.

M. Graham croit que le style normal des systèmes de commandement et de contrôle du gouvernement fédéral n'est pas adéquat pour assurer le partage d'information et des approches communes. Il préfèrerait qu'Ottawa implique de véritables opérateurs d'IE dans cette tâche et non uniquement leurs organisations. M. Graham veut élargir l'implication de la police locale et intégrer la production de rapports sur les IE dans les systèmes existants de surveillance policière.

M. Graham préfèrerait voir des améliorations à la sécurité des infrastructures mises en place de la même façon, par l'entremise des postes de police locaux. Il souhaite toutefois que le gouvernement fédéral joue un rôle plus grand par la création d'une Commission sectorielle sur les IE qui encouragerait la recherche et la formation, par le financement de centres d'excellence non gouvernementaux pour développer le savoir et les capacités, et par le développement et la mise à l'essai d'études de cas et de scénarios de risque en situation réelle. Il encourage le recours à des incitations fiscales pour promouvoir la protection des infrastructures essentielles.

Cinq auteurs partagent le point de vue selon lequel le gouvernement fédéral doit procéder à des changements fondamentaux dans son approche envers la sécurité des IE.

Ces cinq auteurs partagent le point de vue selon lequel le gouvernement fédéral doit procéder à des changements fondamentaux dans son approche envers la sécurité des IE, mais leurs perspectives divergent sur les autres aspects de la question.

MM. Farson, Bland et Cox préconisent tous une expansion formelle des activités du gouvernement fédéral dans ce domaine et leurs recommandations vont de l'établissement formel d'une nouvelle agence à des appels moins précis en faveur d'un leadership national accru, en passant par la tenue de conférences nationales pour établir un nouveau procédé fédéral. Les solutions offertes par MM. Cooper et Graham mettent davantage l'accent sur le travail sur le terrain, avec une responsabilité dispersée dans les postes de police locaux pour la surveillance et la protection des IE et, dans le cas de M. Graham, dans les universités et une Commission pour les IE.

See http://www.macdonaldlaurier.ca/files/pdf/Canadas-Critical-Infrastructure-When-is-safe-enough-safe-enough-December-2011.pdf.

INTRODUCTION[1]

Canada's critical infrastructure (CI) is massive, geographically dispersed, owned by many different players mostly within the private sector, and vulnerable. However, the degree to which that vulnerability transfers into actual risk varies and is clearly in question.

According to the *National Strategy for Critical Infrastructure*,[2] CI is made up of a series of systems vital to the well-being of Canadians. It defines CI as "those physical and information technology facilities, networks, services and assets, which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada."

Canada's CI is dispersed yet interconnected, so applying any simple form of governance to protect it will not work.

Canada's CI is dispersed yet interconnected, so applying any simple form of governance to protect it will not work. This is a unique policy and operational challenge, not just for government, but also for all stakeholders. It cannot be said that we have a fully protected CI, but it also cannot be said that we have one under active threat. What is missing is a cohesive and sustainable approach led by the federal government, with a healthy recognition that such leadership cannot carry the full responsibility for either identifying threats and risks, or doing something about it. That responsibility lies in many hands.

While much is made of the physical components of Canada's CI, there are two other elements connected to the physical components and key to its operation: the cybernetic and the human. There is a growing recognition that CI operators are increasing their dependence on vulnerable remote sensor and control systems. This research effort did not, however, find evidence of the recognition of the human dimensions to CI and its protection. The most notable aspects missing are the relatively small pool of experts who know how systems work and interact as well as the need for continual personal communication within CI systems to maintain a mature and balanced view of risk.

Research to date would indicate that the federal government, while trying to provide a form of general leadership and sharing platforms, lacks most of the policy and operational clout to impose solutions, even when they are known. It therefore tries to provide leadership in partnership with many actors, a nascent effort. The conclusion, therefore, is that Canada's CI is hardly fully safe from incursion, that making it so would involve enormous costs, that the degree of real and present risk is contestable, and, most concerning, that the interdependence of CI systems is developing an overlay of what might be called the meta-CI system, cybernetics, and the computer control systems that control most of the other CI systems such as energy, transportation, finance, and others.

Before jumping to conclusions about the need for more government action, we must give serious thought to what is a reasonable level of response, especially to threats that are potentially devastating but relatively remote. Finally, while efforts exist to improve the protection of CI from attack, we know of very little effort to establish the post-failure resilience of such systems.

The original paper on CI threats concluded with a number of suggestions for ensuring a more secure and sustainable approach to them:

- Understanding that this is a policy mash-up that entails many actors with dispersed responsibilities and that this context will likely not change in the near future;
- Accelerating the slow pace of developing the federal leadership role in information exchange and building communities of practice;
- Adopting a more holistic view of the threats to CI that gives greater emphasis to actual on-the-ground threats such as theft, cyber-incursion, and domestic criminal actions, as well as developing a better understanding for all players of the real risks those threats pose;
- Recognizing the emergent vulnerabilities posed by cybercontrol systems and ensuring an appropriate response; and
- Developing means of sharing information, expertise, and practice that will create a culture of mindfulness shared by all players at all levels.

Some of the key elements needed to meet these objectives are:

- A common understanding of the threats and risks that drive mitigation in both the public and private sector;
- Intelligence effectively shared and applied;
- Adequate reinvestment in CI to avoid increasing its vulnerability through neglect;
- Adequate response capacity suited to the task;
- Continuous updating, sharing of information, learning, and assessment;
- Effective governance within sectors and at the broader national level;
- Public awareness and education to define realistic risks ensure public engagement in the protection of structures vital to its interest and to contain alarmist or ill-informed fears and misunderstandings;
- Ways to provide incentives for the private sector to invest in CI protection; and
- Addressing the human dimension, in that systems can only work reliably when the personnel are equipped with the requisite skills, information, and tools to hold them together.

This paper gathers the thoughts of five scholars who, from differing areas of expertise and experience in their approaches to the vulnerability of Canada's critical infrastructure, discuss the problem, and offer additional directions that may be pursued in attempting to solve it:

STUART FARSON
SIMON FRASER UNIVERSITY

The central question facing those who want to make Canada's critical infrastructure safer concerns how one should look at the issue. Most federal government departments and agencies naturally see the policy dilemmas they face as national ones. Consequently, they seek to develop strategies, plans and programs that satisfy national aims rather than specifically regional or local ones.

In most instances this "one size fits all" approach, with the federal government taking the lead, is a sensible one. It helps keep costs down and its offers the possibility of equality in the provisions of services to the various regions of Canada, both important policy criteria. It is not, however, appropriate for Canada's critical infrastructure. Earlier research suggests it may even cause resentment at the local level.

Planning primarily for resiliency, rather than protection will arguably offer greater long-term benefits.

Two factors help to explain this. The first concerns who owns, who is responsible for, and who is accountable for the various elements of Canada's critical infrastructure. Ownership is extremely diverse. More than 80% is not in the hands of the federal government. While provincial and local governments own some, the vast majority is in private hands. Furthermore, responsibility and accountability for critical infrastructure is frequently split between several different parties, with no consistency between provinces.

The other concerns perceptions of threats and risks. While an "all hazards" approach is appropriate as a starting point for critical infrastructure security, not all regions of the country face the same concerns to the same degree. What may cause severe damage in one part of the country and have long-term consequences will be of little import in another.

These factors suggest that the federal government should recognize that its planning and emphasis should be concentrated – to a significant degree – at the regional level.

The idea that critical infrastructure can be protected has limited conceptual utility. Just as it is impossible to avoid intelligence failures all the time, so too is it impossible to prevent serious hazards from eventuating and sometimes having devastatingly unexpected consequences for critical infrastructure. The standards that were thought yesterday to offer sufficient safeguards against particular dangers will be supplanted as more extreme events occur. There will always be "new normals."

Planning primarily for resiliency, therefore, rather than protection will arguably offer greater long-term benefits. Such an orientation fits well with the needs of private-sector strategic planning. While protecting assets and thwarting known threats is of course a key and routine objective, determining how to be up and running as quickly as possible when faced with a disaster is essential to corporate success, even survival.

Resiliency also means concentrating on emergency preparedness and focusing on the provision of emergency services. Just as critical infrastructure is widely owned by the various levels of government and the private sector, so too are emergency services. In large part, responsibility for such services rests with provincial, municipal and private sector entities. It is critically important that such services are housed in structures that will survive projected catastrophic events.

Needed upgrades to respond to the "new normals" will be expensive and may exceed what local authorities can realistically afford without adopting a scheduled approach. Equally important, however, are back-up plans to provide such services should local authorities be unable to cope. Such plans need a coordinated approach that encompasses all levels of government, the private sector and non-governmental organizations. The various levels of governments have critical roles to play in these regards, particularly concerning the regulation of response requirements to such events as hazardous spills and setting building codes.

It would be wrong, however, to assume from this context that the federal government should perform a mainly secondary role. Where events exceed the capacity of a provincial government to respond, the federal level has a crucially important practical role to play in providing aid to both the civil power and the civil administration. In this regard it will also have an important coordinating role between the entities involved and between the various elements of the federal government that can provide the necessary assistance.

Where events exceed the capacity of a provincial government to respond, the federal level has a crucially important practical role to play in providing aid to both the civil power and the civil administration.

Arguably, the federal government also has a significant part to play in collecting and disseminating the latest thinking about critical infrastructure protection and resiliency. Equally important is the service it can provide regarding the collection, analysis, and dissemination of information and intelligence about the threats and risks that Canada's critical infrastructure potentially faces.

Initially, most of this information was produced by ITAC – then called the Integrated Threat Assessment Centre – and disseminated to the various owners of critical infrastructure by the RCMP in a sanitized form. This strategy had much to commend it. ITAC brought together personnel from across Canada's security and intelligence networks to collate and assess the information to create an all-source product. The RCMP was the logical disseminator, because it has a wider variety of regular contacts than any other federal institution and, besides being the federal police force, it operates under contract to several provinces and numerous municipalities. More recently, ITAC was renamed the Integrated Terrorism Assessment Centre, which indicates its current emphasis.

It is important that the information disseminated to the owners of critical infrastructure does not merely focus on the threats and risks that come to the top of minds today, but adopts a truly all-hazards approach that engages in "over the horizon" scanning. Even in its early days, ITAC's product was considered to be of limed value to consumers of critical infrastructure. It was perceived as being too tactical and not sufficiently strategic to aid in their annual planning cycles. And, significantly, it built no feedback loops into the process to help guide what consumers actually needed. In several instances, more useful information came from critical infrastructure counterparts south of the border. The federal government also has to concern itself with the protection and resiliency of its own institutions. Not only does it need to ensure that it has appropriate planning in place to cover the security of its various entities across the country, but it also has to plan for the transfer of governance from Ottawa should that be necessary.

There is evidence that much critical infrastructure is interconnected with that of the United States. Consequently, what happens to their infrastructure can have immediate consequences across Canada.

The federal government has an important leading part to play in developing and forming formal critical infrastructure agreements with the United States. But other parties, such as the various individual Canadian provinces, their tangential U.S. border states, and the cross-border associations representing infrastructure owners, will also be involved in developing such arrangements. While it is necessary to be cognizant of, and responsive to, the threats that the United States faces, it should not be presumed that these will be replicated to the same degree throughout Canada.

What perspective should the federal government adopt regarding critical infrastructure security? It needs to establish a bifurcated federal agency with much greater presence and resources than currently exist. One part should be decentralized and focus on the regions of Canada and the problems they potentially face. Approaches to critical infrastructure resilience and protection should be developed at this, not the national level, and in close conjunction and cooperation with regional parties. The emphasis should be: "How can we help?" Feedback loops will be essential. The other part should focus on key federal government responsibilities: the security of federal assets, negotiations and development of arrangements with the United States, and how to respond to events beyond provincial capacities.

The emphasis should be: "How can we help?

Stuart Farson is an adjunct professor of political science at Simon Fraser University. He served as research director for a parliamentary committee reviewing the *Canadian Security Intelligence Service Act* in 1989-90, has worked with research institutes in Europe, North America and the Pacific Rim, testified before numerous parliamentary committees, and acted as an adviser to Canadian government and NATO task forces and workshops. He is the author of numerous articles and book chapters on security and intelligence, and he co-edited *Security and Intelligence in a Changing World: New Perspectives for the 1990s*, *Intelligence Analysis and Assessment* and the *PSI Handbook of Global Security and Intelligence: National Approaches.* His latest co-edited book (2011) is *Commissions of Inquiry and National Security: Comparative Approaches.*

DOUGLAS BLAND
QUEEN'S UNIVERSITY

Canada does not have a national critical infrastructure (CI) strategy. This central national security issue is dependent on a weak, incoherent federal "framework document" developed by Public Safety Canada meant to guide a plethora of conflicting authorities if they decided to produce CI security policies in their jurisdictions, government departments, or private enterprises. There is no reliable mechanism to hold anyone to account for any decisions regarding Canada's CI security simply because no one is accountable for Canada's national CI security.

The present federal CI non-policy, non-system cannot be tweaked; it must be entirely invented. This construction should be built on a foundation composed of three conceptual and structural elements:
(1) direct federal government leadership in matters of national CI strategy, security, policy, and management, (2) a CI assessment process refocused from "risk-based analysis to" "vulnerability-based analysis", and (3) a federal government constructed regime of principles, norms, and processes to direct the development and management of a national CI security strategy.

The present federal CI non-policy, non-system cannot be tweaked; it must be entirely invented.

Active National Leadership For CI Security

Public Safety Canada manages a complicated network of "partnerships", including the 14 federal government departments with CI responsibilities, and suggests to these partners that the government's CI "guidelines" would be useful if they were interested in developing CI security programs in their own jurisdictions or industries. Incredibly, the government of Canada does not even have a standard list of terms and definitions to guide CI policy development within its own departments and agencies.[1]

The federal government's general explanation for this abdication of responsibility is that, when CI is defined broadly, it encompasses so many facilities, situations, and programs inside and outside of government that it would be impossible for officials to design a comprehensive, federally directed program. The argument is supported by the assertion that the federal government does not have the authority to dictate CI security terms to provincial and territorial governments or to private business owners. However, the federal government could intervene in CI several matters that touch directly on standing federal government areas of responsibility that are creating policy impediments, as it does in a host of inter-governmental policy areas.

The federal government could lead by example if it were to direct its departments and agencies to develop credible CI security plans in accordance with CI protection standards developed by the federal government. It could also control the scope of the CI management

[1] Canada, Public Safety Canada, "It should be noted that these terms are not intended to define how the various elements interact and/or are assessed, nor is it a Government of Canada standard. Rather, they are common definitions chosen for clarity in order to provide a common language across diverse disciplines." Annex A: Terms And Glossary

problem by establishing, after careful CI assessments based on credible criteria, degrees of infrastructure of "criticality" to national security. Such a scale would relieve the CI policy process of much of its burden and focus the government's attention on truly critical infrastructures.

A National Regime for CI Security

Coherent public policy rests on regimes of principles, norms, rules, and decision-making procedures that join practical policy aims to policy outcomes. Canada's present CI security policies have no clear aims, nor any coherent regime to direct strategic aims if they did exist. The first policy step towards the development of an effective national CI strategy is to assemble an inter-governmental agreement on the national regime for the construction, management, and direction of a national CI security strategy.

Canada's present CI security policies have no clear aims, nor any coherent regime to direct strategic aims

A public policy regime for national CI security must address at least the following fundamental questions:

- What facts and circumstances define a specific infrastructure as "critical"—and to what degree—and thus in need of security?
- What criteria define CI as "secure"?
- To what degree do "national security considerations" override provincial and territorial and private enterprises' rights to build and manage infrastructure that serves the public?
- Who among the three levels of government decides who pays and who gets what in matters of national CI security?
- What regulatory instruments need to be developed to manage and support a national CI security strategy?

From "Risk-Based Analysis" to "Vulnerability-Based Analysis"

Canada's assessments of CI security as described in a convoluted and internally confused Public Safety Canada statement is centred on "risk-based analysis" aimed at "… clarifying the dimensions of risk [to every CI in Canada] including its causes, likelihood of occurrence and possible severity of consequences."[2] Yet risk is inherent in every element of CI, from development to installation to daily operation. Threats are as innumerable as imagination allows. Policies, therefore, based on attempting to guess what present and future risks might be and how they will unfold and with what consequences, are sure to be overcome by necessarily narrow analysis (can anyone really account for every risk facing even minor CI systems and circumstances?) and 9/11-type surprises.

It is possible to know with a high degree of certainty where the weaknesses and vulnerabilities lie in each CI system, and then to develop and implement plans to reduce system vulnerabilities or to regenerate systems in cases of failure. It is also possible to assess the "cost-efficiency" of CIs and CI systems and then to determine their criticality to Canada's well-being. It is possible to improve the security of critical structures and systems if governments and private enterprises begin the process from a sound, coherent conceptual framework.

The central CI policy question is not, "What risks lie in wait?" but "To what degree and cost is Canada's security and social, industrial, and economic welfare vulnerable to a disruption to a particular CI or critical system no matter the cause or source of that a disruption?"

[2] Ibid, Section 4.2.

The critical component of a CI is not its physical structure, but the products and services the structure delivers to the public that are critical to public safety and well-being. The primary aim of a CI security strategy, therefore, must be to ensure the continued delivery of essential products and services to governments and Canadians in the event that a particular CI system is disabled.

In the case of a particular CI, the answer derived from vulnerability-based analysis determines whether or not it is secure. Officials can then prepare appropriate, practical responses to safeguard the products the CI delivers to Canadians.

The primary aim of a CI security strategy must be to ensure the continued delivery of essential products and services to governments and Canadians in the event that a particular CI system is disabled.

A CI security regime aimed at mitigating service vulnerabilities requires the development of an inventory of CI systems, an assessment of the social, industrial, and economic value delivered by each CI and each system, and an assessment of the social, industrial and economic costs of any event – accidental, natural, or hostile – that might degrade each CI or system.

A Summary of Recommendations

The federal government should develop, direct, and manage a comprehensive, government-wide policy to protect federal, provincial, local, and private infrastructures it deems critical to the security, safety, and social and economic welfare of Canada and Canadians. In order to do this, we need an inter-governmental convention to establish a national CI regime to create the policy. All levels of government and private industry should cooperatively develop a vulnerability-based analysis program as the central pillar in assessments of Canada's national CI security needs, and then CI vulnerability reduction programs. These programs might include establishing high-grade physical secure measures for some systems; creating system redundancies; creating alternate sources or means to provide for essential products; and stockpiling essential commodities, among other things.

Douglas Bland earned his Ph.D from Queen's University and is a Professor and Chair in Defence Management Studies in the Queen's University School of Policy Studies. His research is concentrated in the fields of defence policy making and management at national and international levels, the organization and functioning of defence ministries, and civil-military relations. Among other works on defence management, he wrote *The Administration of Defence Policy in Canada 1947-84* (1987) and *Chiefs of Defence: Government And The Unified Command of The Canadian Armed Forces* (1995).

BRIGADIER-GENERAL JAMES COX (RETIRED)
MACDONALD-LAURIER INSTITUTE

Professor Andrew Graham's "Canada's Critical Infrastructure: When is Safe Enough Safe Enough?" describes a number of policy challenges facing the federal government in the field of Critical Infrastructure Protection (CIP). However, to be of any use, CIP policy must be manifest in action and it is in this particular area that the federal government seems to lack leadership.

The federal government – like provincial and territorial governments – has clear responsibility for and direct authority over the few critical infrastructures (CIs) they own, but about 85 percent of CI in Canada is owned and operated by the private sector. Within the private sector, there is palpable discontent over the lack of robust federal government leadership of efforts to enhance Canadian CIP programs.

Within the private sector, there is palpable discontent over the lack of robust federal government leadership.

In a 2006 paper for the Canadian Centre of Intelligence and Security Studies in the Norman Paterson School of International Affairs, John Hay argues, "protecting critical energy infrastructure … is an inescapable element of the national interest, and of the public interest." If he is right, then government should follow the earlier advice of Simon Fraser University's Dr. Stuart Farson.

In 2004, Dr. Farson, one of Canada's foremost intelligence scholars, wrote an opinion for the federal government explaining his views on the implementation of the 2003 *Anti-Terrorism Act*. Farson argues that the private sector has a primary responsibility both for thwarting threats and for making their CI assets resilient against them. Therefore a critical need exists to share information and intelligence among the various levels of government and the private sector, at strategic and tactical levels. Historically however, Canadian intelligence agencies have been reluctant to share information not only with provincial and municipal governments, but with the private sector as well. This reluctance continues today.

Within the CI private sector, Francis Bradley is Vice-President of the Canadian Electricity Association and is responsible for the Association's CIP programs. Mr. Bradley laments the federal government's failure to establish a formal information-sharing framework to facilitate the necessary two-way flow of information and intelligence between the public and private sectors. As a result, both suffer. One on hand, CI industries and businesses do not get the situational awareness of the threat environment needed to determine appropriate operational postures. On the other hand, without a two-way information flow, how can government provide an accurate picture of the threat environment when it is blind to what is occurring in up to 85 percent of critical facilities and systems?

Reluctance to share information and intelligence is evident mainly at the federal level. According to Bradley, in most jurisdictions information flows much more freely at lower levels. Local initiatives and informal relationships forged between individuals who know each other have stimulated cooperative information and intelligence exchanges that result from a willingness to "get on with it" at the working level, rather than simply sitting back and waiting for federal government direction. Ultimately, the private sector wants a broad, formalized information-sharing framework at the national level so that complementary local level practices can be formalized, too.

Reluctance to share information and intelligence is evident mainly at the federal level.

Academic experts also see problems with federal government leadership. Dr. Wayne Boone, Coordinator and Principal Instructor of the Master of Infrastructure and International Security (MIPIS) Program at Carleton University, is one of Canada's new emerging CIP experts. Dr. Boone comes down hard on the lack of determined policy and strategy *action* by the federal government. One of his principal complaints is that the public service generalists who write CIP policy and strategy have little operational experience in the subject. He contends that working level CIP "operators," who are knowledgeable and experienced, are not adequately consulted by bureaucrats.

Bradley offers a practical example of this problem. It seems government offices in Ottawa routinely ask for simple "lists" of CIs from private-sector stakeholders, but those offices do not seem to understand that "criticality" is circumstantial, changing with time, threat, business, and operational requirements; circumstances are not truly known until all salient information and intelligence is made available.

"Criticality" is circumstantial, changing with time, threat, business, and operational requirements.

This lack of government "grip" on CIP complexity is apparent in the federal government's *National Strategy for Critical Infrastructure* (NSCI). It is a passive document that doesn't really *do* anything. There is no mention of national standards or enforcement measures. There is no mention of strategic priorities. In fact, as written, it simply implies that all levels of government and private owners of CIs should work together to pick up the pieces as best they can *after* a debilitating CI event.

The need to protect the 85 percent of CIs owned by the private sector is in the Canadian national interest. This issue represents the centre of gravity of CIP in Canada. The main conclusion to be drawn from Professor Graham's paper and other related views found here is that the federal government needs to *do* more to engage the private sector. Two things in particular need to be done.

First, the federal government should lead from the front and exercise a more robust, proactive approach with private sector CI industries, businesses, professional associations, and academia. In addition to the current loose arrangements for sectoral consultation, a more structured, formal relationship should be established, featuring meaningful consultation by all government departments having a CIP responsibility. A corollary would call for increased participation of the private sector in regular government CIP training and exercises as part of the overall emergency measures exercise program.

Second, the centerpiece of this enhanced relationship would be a structured information and intelligence-sharing regime. There are challenges here to be sure, but the status of CIP as a national interest demands that all stakeholders be treated with the appropriate degree of respect and trust if they are to be imposed upon to participate in the protection of Canadians and the defence of our way of life.

The federal government should lead from the front and exercise a more robust, proactive approach with private sector CI industries, businesses, professional associations, and academia.

The federal government needs to move beyond bland pronouncements and unfunded CIP strategies. It needs to *do* things and inspire others to follow. Federal government CIP leadership needs some energy.

James Cox is a Veteran and former Brigadier-General in the Canadian Forces with over 35 years experience in operational command and staff appointments across Canada and abroad with NATO and the U.N. Until last May, he served as a parliamentary analyst for six years, advising parliamentary committees on issues of national defence and veterans' issues. He now teaches Canadian foreign policy at the University of Ottawa and civil-military relations at the Norman Paterson School of International Affairs at Carleton University. He is also a Senior Fellow of the Macdonald-Laurier Institute.

BARRY COOPER
UNIVERSITY OF CALGARY

Geopolitics underlies the problems of safety in Canadian CI and conditions any plausible response to them. First, by far the greatest threats are natural disasters, especially floods, storms, and, at least in the Lower Mainland of BC, earthquakes. Human threats are "latent" rather than real. Second, most Canadian CI is in private hands – 85 percent by one estimate. As a result, the focus of the owners of Canadian CI is more on accidental damage, aging physical plants, and vandalism than it is on terrorism and catastrophic failure.

For example, the most likely threat to Canadian energy pipelines comes from digging at construction sites, not sabotage. Due to widespread private ownership, there is an understandable reluctance to share information with governments that do not place the same value on proprietary information as do its owners. As a result of the importance of energy-related CI, and the way, for example, pipelines are monitored, namely by remote computerized sensing and control systems, the real human threat (such as it is) may better be understood in terms of cyber attacks than shifting landforms or kinetic attack. In other words, cyber threats can be seen as "meta-threats," that is, both a direct and an indirect threat. This is a point to which we return below.

A risk-free society is not possible because risk is inherent in the human capacity to act.

Canadian CI is vulnerable because it is dispersed and its vulnerability matters because CI is important. But vulnerability does not necessarily mean our CI is at risk, but only that it might be. In order to be at risk, CI must be threatened and the threats must be assessed in terms of credibility or probability as well as severity of the potential for damage. A clear understanding of the trade-offs between low-impact and high-probability events (such as pipeline rupture) and low-probability, high-impact ones (such as cascading electrical failures) is necessary in order to allocate our limited threat-prevention and threat-mitigation resources. Such allocations invariably involve political decisions pressured by regionally competitive interests and the unavoidable question of federalism and shared jurisdictions.

A problem that renders the questions of limited resources and federalism even more difficult is that the seemingly commonsensical question "Are we safe enough?" is not appropriate, chiefly because it cannot be answered. A risk-free society is not possible because risk is inherent in the human capacity to act; the attempt to create a risk-free society is not desirable because the cost in hard cash is infinite. Moreover, the effort to create such a political order is self-destructive because it invariably extinguishes individual liberty. Accordingly, the problem of vulnerability needs to be rearticulated in terms of resiliency, not complete protection or security. As a consequence, the role of government, especially the Government of Canada, is necessarily more limited than Ottawa bureaucrats typically allow.

Specifically, the reliance of the Government of Canada on what they call "all hazard [or all threat] risk analysis" needs to be reconsidered in light of: (1) the limited jurisdiction of the Government of Canada, and (2) the limited capacity of any government to deliver "security." As Graham pointed out, such an approach is defensive and so reactive rather than proactive, statecentric when the state is in many respects peripheral, and complex beyond the capacity of even the cleverest bureaucrat to comprehend. Such a strategy ensures defeat because its goals are impossible to achieve.

As a consequence, most state activity, especially by the Government of Canada, is nothing but planning to plan. This is a bureaucratic nightmare because Public Safety Canada must attempt to coordinate its activities with fourteen other departments and agencies, which is a recipe for the kind of disaster that the American Federal Emergency Management Agency experienced in its response to Hurricane Katrina. In short, non-recognition of reality with respect to security, which we may choose to label "federal leadership," is likely to mean the issuing of ineffective and largely harmless rules by remote bureaucrats, not effective political responsibility.

The Government of Canada might play an effective role—possibly by restoring the RCMP Commercial Crime Unit to an elite formation within the organization in the area of cyber threats and cyber crime.

So long as Canadian CI is widely distributed and so long as Canada is governed as a federation, it is useful to think of distribution of CI and responsibility for its protection as two sides of the same coin. Indeed, diffused CI can be seen as a strength because it makes coordinated attacks more difficult and because diffuse responsibility, besides reflecting the constitutional order of the federation, allows local authorities to exercise their proper responsibilities. Moreover, the existing links between privately owned CI and local police and other first-responders means that the fantasy of centralized coordination (or rather, duplication of existing protocols) by Public Safety Canada must be abandoned.

There is one area where the Government of Canada might play an effective role –possibly by restoring the RCMP Commercial Crime Unit to an elite formation within the organization in the area of cyber threats and cyber crime. Cyber threats are inherently novel and changing, chiefly because they rely on innovative and emergent technologies, from social media and botnets to cloud computing and constant connectivity. The Pentagon established Cyber Command as a subordinate command to Strategic Command in 2009 precisely to deal with military threats from cyber space. In early 2011, a Chinese-based cyber attack on Treasury Board and the Departments of Finance and National Defence indicated that it would be prudent to follow the American example.

Moreover, as noted above, any threat to energy CI is better conceptualized as a cyber threat to management of operations than as a direct or kinetic threat to disrupt them. If there are to be any useful initiatives by the Government of Canada besides the churning out of ever more elegant plans, cyber threats would be a good place to start.

Barry Cooper received his Ph.D. from Duke University and is a professor at the University of Calgary. He has taught at Bishop's University, McGill, and York University. For the past twenty-five years, he has studied western political philosophy, both classical and contemporary. Cooper's other area of continuing interest has been Canadian politics and public policy. Here he has brought the insights of political philosophers to bear on contemporary issues, including the place of technology and the media in Canada and the precarious status of Canadian defence and security. He is the author, editor, or translator of 27 books and has published over 130 papers and book chapters. He writes a weekly column in the *Calgary Herald*.

ANDREW GRAHAM
QUEEN'S UNIVERSITY

Over the course of my research into critical infrastructure (CI), I heard many times: "It is going to take a disaster to make us take this seriously." I do not buy that. What a disaster will probably show is that, in both government and the infrastructure industry, much has been done.

These efforts are co-ordinated lightly. The federal government focuses on higher level, low-probability risks, while serious vulnerabilities and more active risks that are less interesting, more real, and more deadly are given less attention. Between government and industry, the sharing of information and common approaches are sadly lacking. This is the standard lay-put of the findings of public enquiries into matters of this kind.

Solutions of the command and control kind will only go so far in this highly distributed environment. We must cajole, engage, and entice. The following are some of the steps that need to be taken to develop a system-wide capacity to identify CI risks, engage the right players in action, and build resilient capacity:

- Expand the Risk Process: Move risk assessment out of the current closed-loop environment through more open risk identification sessions with players at all levels across the country. Clearly, work has to be done to separate inherent threats from the real risks of actual attack, breakdown, or control failure. These must be broken down into digestible chunks: national, regional, and local, all graded with respect to severity and likelihood, all updated regularly. Above all, such a system should be credible, made so by solid analysis, language that informs but does not incite, regular and consistent updates, and the correction of errors once learned.

Between government and industry, the sharing of information and common approaches are sadly lacking.

- Bring In Operators, not just Organizations: Engage actual CI operators and their internal expertise, not just their representative national organizations. Such engagement would be separate from the formal communications efforts currently in place. Rather, it would be part of the risk identification and assessment process. It would also be part of the skills development process supported by the proposed CI Sector Council. As such, it would take a third party entity to make it work over time. That could be a combination of the Sector Council and the research centre(s) proposed below.
- Localize Police Involvement: Expand police involvement beyond the national institutions with their focus on terrorism to both provincial and municipal services. Local services are often attuned to other threats and risks such as vandalism and theft that can have equally devastating impacts on CI.
- Avoid Isolated Reporting Channels and Get on Board with Analytics: Integrate CI reporting in existing police intelligence systems. Current efforts to develop special reporting of CI threats will die if they depend on police reporting separately and not through the rapidly developing local analytic systems local police services are creating. Such systems are forcing the integration of information about crime, locale and participants in new ways. Current efforts to have CI incidents reported on their own track flies in the face of the potential for analytics to provide key insights about the nature of threats in specific communities.

- Centres of Excellence: Invest in continuing research by establishing independent centres of excellence in universities to build knowledge and capacity. It has been clear throughout the preparation of this paper that there is not a great deal of research into CI risks, risk techniques, comparative analysis of activities in other countries, and the examination of the field that is much needed.
- CI Sector Council: Develop a CI Sector Council similar to those developed for the policing sector to foster thinking, research, and action in the human resources elements of building CI capacity throughout the system. This has included the identification of core competencies, common training, and the professional development of key personnel.
- Tax Incentives: Develop more incentives for the CI industry to invest in building both protection and response capacity through tax incentives based on capital investments and training for staff. This is easier said than done, but well worth pursuing as a medium-term objective. What is clear is that such incentives are preferable to a public expenditure program.
- Test Scenarios in the Real World: Through Public Safety Canada, funded centres of excellence, and with CI industry partners, develop test scenarios for individual targets as well as regions potentially affected by CI failure. These must be fulsome and complete, in that they cannot be simply those inside the system talking to those inside the system. CI failure is a social phenomenon that, when it happens, engages society fully. Therefore, such testing must engage communities in different ways. For example, it is impossible to consider a CI failure in power without involving policing, health, municipal services, and transportation services. Hence, the mantra of all hazards must be taken seriously.

Move risk assessment out of the current closed-loop environment through more open risk identification sessions with players at all levels across the country.

- Build Case Studies to Share Knowledge: Develop learning tools, not just incident reports and enquiries. To do this, a case study program needs to be created that shares knowledge within sectors and across sectors. Case studies are powerful tools for learning in that they provide context, give information about a challenge, what was done about it, and what was learned in the process. All of this is outside the more judgemental and politicized environment of post-incident investigations. In addition, case studies let those with expertise share their experiences with others in a way that suits their culture: through structured stories. Sharing ways to solve problems is a way to prevent them.

In the end, all of these suggestions are aimed at developing a community of practice in a rather disbursed and varied area. There is no one big problem, and there is no single fix. Perhaps the WWII slogan of "Keep Calm and Carry On" needs to be adapted to "Keep Calm and Get on with It."

Andrew Graham is an adjunct professor at Queen's University's School of Policy Studies, where he teaches and writes on public sector management, financial management, integrated risk management, and governance. He has a Master of Arts degree in Political Economy from the University of Toronto and a B.A. from Glendon College, York University. He is a graduate of the Advanced Management Program of the Canadian Centre for Management Development. Professor Graham has over thirty years of experience working in the public sector, including 14 years as an assistant deputy minister in the federal government.

CONCLUSIONS

Although the five scholars who contributed to this symposium may disagree about the structure of solutions to the problem of the vulnerability of Canada's critical infrastructure, they do so from a fairly uniform position about the nature of the problem. They agree that the federal government's approach to date has been inadequate, especially in terms of informing stakeholders about the risks we face.

The problem they unanimously condemn is the proclivity of federal governmental entities to silo information and their seeming inability to develop structures for the fulsome sharing of knowledge of threats and possible strategies to address them. A common theme that emerges from their work is that the dispersed nature of knowledge and utilization of it throughout Canada's critical infrastructure require imaginative new policies that links stakeholders with informational tools that can help them understand, manage and contain risk.

The real measure of the strength of our critical infrastructure awaits the natural or manmade catastrophe that will test it.

They differ on the nuts and bolts. Do we need a new national agency, whether its role is simply to act as a clearing house for information or the proactive enforcement of uniform codes and standards? Is the federal government capable of changing its own culture and offering leadership that is effective? How real is the risk, and how can we best deal with it? In these respect, our writers agree on little.

Of course, as in all complicated matters of public policy, the real measure of the strength of our critical infrastructure awaits the natural or manmade catastrophe that will test it. In the meantime, to paraphrase Andrew Graham, our key players should "Keep Calm and Get On With Improving It."

ENDNOTES

1 This section is adapted from the executive summary of *Canada's Critical Infrastructure: When is Safe Enough Safe Enough?,* by Andrew Graham, published by the Macdonald-Laurier Institute in December, 2011, see http://www.macdonaldlaurier.ca/files/pdf/Canadas-Critical-Infrastructure-When-is-safe-enough-safe-enough-December-2011.pdf.

2 See http://www.publicsafety.gc.ca/prg/ns/ci/ntnl-eng.aspx.

THE MACDONALD-LAURIER INSTITUTE

True North in Canadian Public Policy

The Macdonald-Laurier Insitute for Public Policy exists
to make poor-quality public policy in Ottawa unacceptable
to Canadians and their political and opinion leaders,
by proposing thoughtful alternatives through non-partisan
and independent research and commentary.

The Macdonald-Laurier Insitute is an independent, non-partisan registered charity for educational purposes in both Canada and the United States. We are grateful for support from a variety of foundations, corporations and individual donors. The Institute would not be able to continue making a diffrence for Canadians without the support of people across Canada and the United States for our publications on policy issues from aboriginal affairs to democratic institutions; support for our events featuring thought and opinion leaders; and support for our other activities .

For information on supporting the work of the Macdonald-Laurier Insitute
by making a charitable donation, please visit our website at
www.macdonaldlaurier.ca/supportMLI

The notion that a new think-tank in Ottawa is unnecessary because it
would duplicate existing institutions is completely mistaken. The truth is
there is a deep dearth of independent think-tanks in our nation's capital.
- Allan Gotlieb, former Deput Minister of External Affairs and
Ambassador to Washington

To surmount the enormous challenges of getting Canada's place
in the world right and taking advantage of changing opportunities,
we need more ideas, input, discussion and debate in Ottawa - that
is where the crucial decisions about our future are made.
That's why MLI is so vital to Canada today.
- Hon. James S. Peterson, former Minister of International Trade
and Member of Parliament for 23 years

MLI is a registered charity for educational purposes with the IRS and CRA

Making a Name for Ourselves!

N

MLI

Sir Antony Fisher
International
Memorial
Awards

Winner, Sir Antony Fisher International Memorial Award
Best Think Tank Book in 2011
as awarded by the Atlas Economic Research Foundation

"Top 20 New Think Tank" in the world for 2010
as rated by the University of Pennsylvania

What people are saying about MLI:

Very much enjoyed your presentation this morning. It was first-rate and an excellent way of presenting the options which Canada faces during this period of "choice." ... Best regards, and keep up the good work.

Preston Manning, President and CEO, Manning Centre for Building Democracy

Congratulations all for the well deserved recognition. You've come a long way in a very short period of time.

Marc Patrone, Commissioner, CRTC

The reports and studies coming out of MLI are making a difference, and the Institute is quickly emerging as a premier Canadian think tank.

Jock Finlayson, Executive Vice President of Policy, Business Council of BC

In the global think-tank world, MLI has emerged quite suddenly as the "disruptive" innovator, achieving a well-deserved profile in mere months that most of the established players in the field can only envy. In a medium where timely, relevant, and provocative commentary defines value, MLI has already set the bar for think-tanks in Canada."

Peter Nicholson, former senior policy advisor to Prime Minister Paul Martin

Where you've seen us:

THE GLOBE AND MAIL

NATIONAL POST

FP Foreign Policy

THE WALL STREET JOURNAL.

HILL TIMES

The Economist

and in other major Canadian and international media

www.macdonaldlaurier.ca

MLI