CANADA'S CRITICAL INFRASTRUCTURE

When is Safe Enough Safe Enough?

Andrew Graham

2 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 (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. Our 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.

Canada's critical infrastructure (CI) is massive, geographically dispersed, owned by many different players mostly within the private sector, and vulnerable. Applying any simple form of governance to protect it will not work.

According to the *National Strategy for Critical Infrastructure*,[1] 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."[2]

While much is made of the physical components of Canada's CI, there are two others 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,

serious thought has to be given to what is a reasonable level of response, especially to threats that are potentially devastating but relatively remote. Finally, while there are efforts to improve the protection of CI from attack, we know of very little effort to establish post-failure resilience of such systems.

The paper concludes with a number of suggestions for ensuring a more secure and sustainable approach to CI threats:

Understanding that this is a policy mash-up that entails many actors with dispersed responsibilities and that it 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 cyber-control 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.

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.

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

- A clear mapping of CI in the country;
- 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.

SOMMAIRE

Les infrastructures essentielles (IE) du Canada constituent un système de très grande envergure, géographiquement dispersé, qui est la propriété de nombreux joueurs situés surtout dans le secteur privé, et qui est vulnérable. Toutefois, la mesure dans laquelle cette vulnérabilité se traduit par des risques réels n'est pas uniforme et doit être au centre de nos préoccupations. Nos IE sont dispersées tout en étant inter reliées, et on ne peut leur appliquer une forme unique de gouvernance pour les protéger. Il s'agit d'un défi opérationnel et de politique unique non seulement pour le gouvernement, mais aussi pour toutes les parties prenantes. On ne peut pas dire que nous avons des IE tout à fait protégées, ni qu'elles sont menacées. Ce qui manque est une approche cohésive et durable menée par le gouvernement fédéral, couplée avec une saine reconnaissance du fait qu'un tel leadership ne peut porter à lui seul toute la responsabilité de déterminer les menaces et les risques, ni de les contrer. Cette responsabilité doit être partagée par plusieurs parties.

Les infrastructures essentielles (IE) du Canada constituent un système de très grande envergure, géographiquement dispersé, qui est la propriété de nombreux joueurs situés surtout dans le secteur privé, et qui est vulnérable. On ne peut leur appliquer une forme unique de gouvernance pour les protéger.

Selon la *Stratégie nationale sur les infrastructures essentielles*,[1] les IE sont composées d'une série de systèmes d'une importance cruciale pour le bien-être des Canadiens. Elle définit les IE comme «.les installations, réseaux, services et biens physiques et ceux de la technologie de l'information, dont la défaillance ou la destruction entraînerait de graves répercussions sur la santé, la sécurité ou le bien-être économique des Canadiens, ou encore sur le bon fonctionnement des gouvernements du pays. »[2]

Bien qu'on discute beaucoup des composantes physiques des IE du Canada, il en existe deux autres qui sont reliées aux composantes physiques et qui sont essentielles à leurs opérations.: les composantes cybernétique et humaine. Il est de plus en plus reconnu que les opérateurs d'IE accroissent leur dépendance envers des systèmes de détection et de contrôle à distance vulnérables. Nos recherches n'ont toutefois pas trouvé d'indices d'une reconnaissance de la dimension humaine associée aux IE et à leur protection. Les aspects manquants les plus notables sont le bassin relativement restreint d'experts qui savent comment les systèmes fonctionnent et interagissent de même que la nécessité d'une communication continuelle entre les personnes au sein des systèmes d'IE pour maintenir une approche mûrie et equilibrée des risques.

La recherche faite à ce jour indique que le gouvernement fédéral, même s'il essaie de fournir une certaine forme de leadership global et s'il partage ses plateformes, ne possède pas l'influence opérationnelle et sur le plan des politiques nécessaire pour imposer des solutions, même lorsque celles-ci sont connues. Il essaie par conséquent de fournir un leadership en partenariat avec plusieurs acteurs, ce qui constitue un début d'effort. Nous devons donc conclure que les IE canadiennes sont loin d'être entièrement à l'abri

d'une incursion, qu'il faudrait investir des sommes énormes pour arriver à cet objectif, que le degré de risque réel est discutable et, ce qui est le plus préoccupant, que l'interdépendance des systèmes d'IE est en voie de développer une nouvelle couche de ce que l'on pourrait appeler le système méta-IE, la cybernétique, et les systèmes de contrôle par ordinateur qui contrôlent la plupart des systèmes d'IE tels que l'énergie, le transport, la finance etc.

Avant de sauter aux conclusions quant à la nécessité pour le gouvernement d'intervenir davantage, il faudrait sérieusement réfléchir à ce qui constituerait un niveau de réponse raisonnable, en particulier aux menaces potentiellement dévastatrices mais relativement éloignées. Enfin, bien que des actions soient en cours pour améliorer la protection des IE contre les attaques, nous n'avons connaissance que de très peu d'efforts pour assurer la résilience de ces systèmes à la suite d'un échec.

Le gouvernement fédéral, même s'il essaie de fournir une certaine forme de leadership global et s'il partage ses plateformes, ne possède pas l'influence opérationnelle et sur le plan des politiques nécessaire pour imposer des solutions, même lorsque celles-ci sont connues.

La présente étude offre en conclusion un certain nombre de suggestions pour s'assurer qu'on confronte les menaces envers les IE de façon plus sécuritaire et durable.:

Comprendre qu'il s'agit d'un amalgame sur le plan des politiques qui implique de nombreux acteurs avec des responsabilités diverses et qu'il est peu probable que cela change dans un avenir proche;

Accélérer le rythme lent de développement du rôle fédéral de leadership dans l'échange d'information et la construction de communautés de pratique;

Adopter une perspective plus holistique des menaces aux IE qui met davantage l'accent sur les menaces réelles sur le terrain telles que le vol, les cyber attaques et les activités criminelles domestiques, et développer chez tous les participants une meilleure compréhension des risques réels que posent ces menaces;

Reconnaître les vulnérabilités émergentes qu'amènent les systèmes de cyber contrôle et assurer une réponse appropriée; et

Développer des moyens de partager l'information, l'expertise et les pratiques de façon à créer une attitude d'attention partagée par tous les participants à tous les niveaux.

Certains des éléments clés nécessaires pour atteindre ces objectifs sont.:

- La confection d'un plan détaillé des IE à travers le pays;
- Une compréhension commune des menaces et des risques qu'on cherche à atténuer autant dans le secteur public que le secteur privé;
- Des renseignements concrètement partagés et mis en application;
- Un réinvestissement adéquat dans les IE pour éviter d'augmenter leur vulnérabilité par la négligence;
- Une capacité adéquate de réponse adaptée à la situation;
- Une mise à jour et un partage de l'information, un apprentissage et une évaluation continus;
- Une gouvernance effective au sein des secteurs et au niveau national;
- Une prise de conscience et une éducation auprès du public sur les risques réalistes pour assurer son engagement dans la protection de structures qui lui sont d'un intérêt crucial et pour contenir les peurs et incompréhensions fondées sur un sentiment alarmiste ou un manque d'information;
- Des façons de fournir des incitations au secteur privé pour investir dans la protection des IE; et
- Une prise en compte de la dimension humaine dans la mesure où les systèmes ne peuvent fonctionner de manière fiable que lorsque le personnel est doté des compétences, de l'information et des outils requis pour leur entretien.

INTRODUCTION

We take them for granted. Canadians expect to pick up the phone and have a dial tone, turn a switch and have power, a ready supply of fuel for a natural gas furnace, to be able to move from one part of the country to another, to turn a faucet for safe drinking water, and to call 911 and receive immediate assistance. Increasingly, Canadians expect to be able to send a text or picture just taken on a cell phone. We expect to do our banking on line, securely and without disruption. We expect a lot, and we get it most of the time.

For the most part, Canadians understand disruptions to these services in a natural disaster. What we also expect is quick restoration of these services. What we ignore is the inherent fragility of the systems that deliver this way of life. We ignore the massive and continuous effort put into making it work almost all the time. We are also not aware of the threats and risks from the human and natural world to those key elements of critical infrastructure that make our lives so comfortable. When something goes wrong, do we ask: are we safe enough?

This monograph will raise a number of questions concerning the built lifelines of Canadian society, their safety, and what we need to do about it in the face of emerging human and natural threats and risks. While answers are readily available, so too are gaps and ambiguities that leave one unsure about that question: are we safe enough? This reflects the state of play in this area today and the need for a larger, balanced, and more open dialogue. While threats exist, many efforts to mitigate them are already under way. That being said, the field is so diverse and complex, no one player can be held to account for the whole. In addition, the traditional response, often characterized by demanding further government action, flies in the face of that complexity. There are too many interests, too widely disbursed, for that sort of solution. In that respect, critical infrastructure safety is a true 21st century problem demanding a complex and multi-party set of solutions. As described below, it fits the emerging definition of a public policy mash-up.

Critical infrastructures (CI) are the key physical, cybernetic, and human systems that sustain our way of life, and are complex, pervasive, and increasingly interdependent. Exploring how they work and their vulnerabilities would take more space than is permitted here. Further assessing security risks and then facing the more daunting tasks of testing their validity will require a restraint that avoids the sensational without sacrificing the need for watchful mindfulness.

What we ignore is the inherent fragility of the systems that deliver this way of life.

CENTRAL TASK AND THESIS

The task here is to describe Canada's CI, identify sources of threat, assess current efforts to address those threats, ask questions that remain to be answered, and suggest themes for moving forward and building on the work that has already been done in government and the private sector.

The central thesis based on the research to date is that ownership of CI is widely distributed and responsibility, in terms of who must lead the overall process, and accountability, in terms of who must ultimately answer for specific results, is diffused. 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 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, serious thought has to be given to what a reasonable level of response is to remote but potentially devastating threats. Finally, while there are efforts to improve the protection of CI from attack, we know of very little effort to establish post-failure resilience of such systems.

WHAT IS CRITICAL INFRASTRUCTURE?

The danger when discussing CI is making it either too broad or too narrow. It is also clear that at times, criticality can be in the eye of the beholder. Little emerges from the research that would indicate that any country has fully defined what is critical and what is not. Further, the issue of what is infrastructure and what is not is moot. Physical assets, for the most part, are readily identified with something approaching consensus. Intangibles and cyber assets are less clear in this context. Finally, the issue of sectoral coverage varies around the world.

The field is so diverse and complex, no one player can be held to account for the whole.

CI assets can be broken down into three broad categories:

1. Physical: These are all the tangible assets such as roads, pipelines, transmission lines, dams, and vital institutions such as hospitals that are deemed essential to maintaining our society. Physically stored information is a part of this category.

2. Cybernetic: This rapidly expanding category includes all the technology that depends upon information hardware software, data, and networks used within the CI context. This also includes all electronic information stored within these systems and controlling and monitoring systems that permit remote management of CI asset components.

3. Human: Often forgotten in this discussion are the people who operate CI systems. They have knowledge, know-how, and experience that, if lost, represents a major threat to the ability to sustain or restore CI systems. Also included are other elements of human threats such as the potential for insider access to physical plant and systems as well as the robustness of management and culture to be alert to threats and build in resilience.

According to the *National Strategy for Critical Infrastructure*,[3] 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."[4]

Within this definition, the government defined 10 sectors:

- Energy and utilities – electrical power, natural gas, oil production and supporting transmission systems, high risk facilities;

- Finance – banking, securities, investments, integrity of electronic banking systems;

- Food – food safety at production, sales and use nodes, distribution;

- Transportation – roads, air, rail, marine;

- Government – services, public facilities, information and information networks, secure and protected sites;

- Information and communication technology – telecommunications, broadcasting, software, hardware, networks;

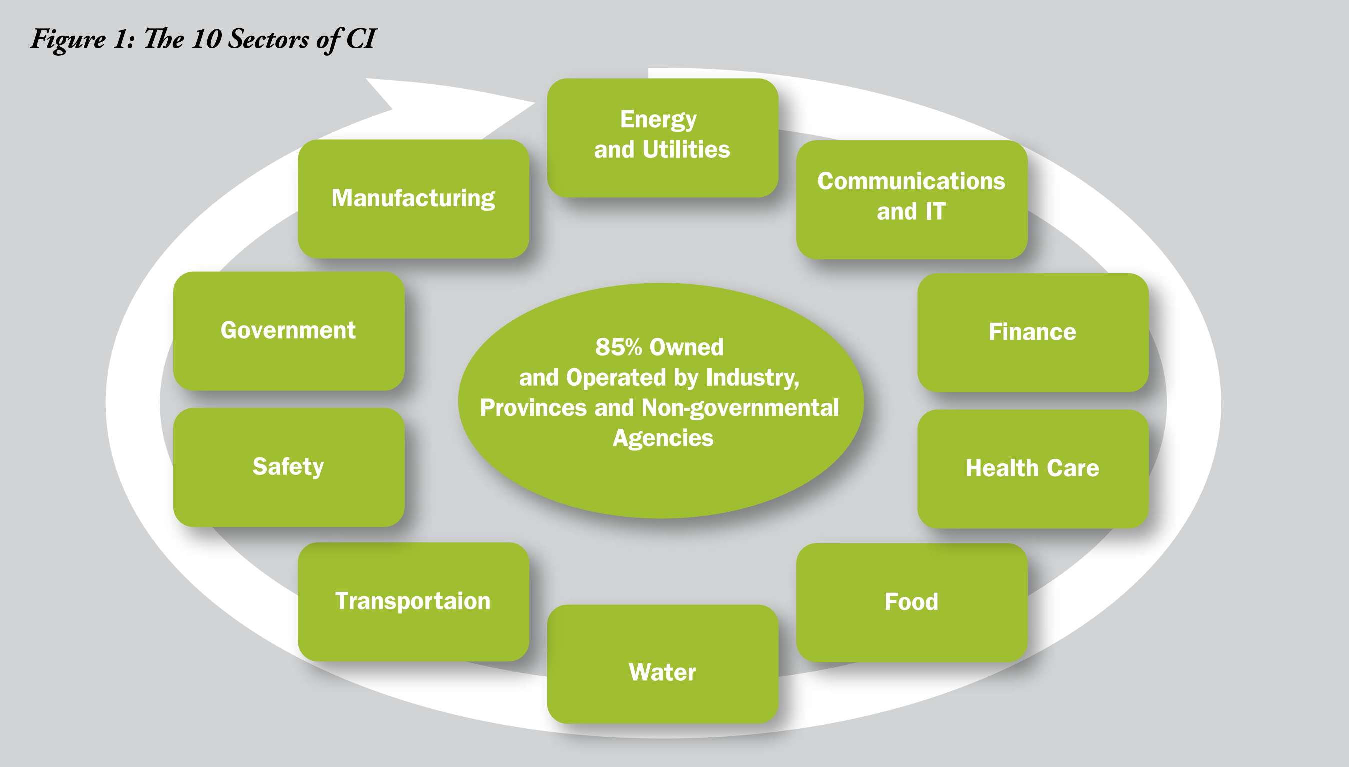
- Health – hospitals, health-care, blood supply;

- Water – drinking water, waste water contamination;

- Safety – hazardous substances, explosives, nuclear waste, emergency services; and

- Manufacturing – chemical and strategic manufacturers.

Figure 1: The 10 Sectors of CI



Several characteristics of this definition are striking. First, it is pervasive. There is little in the daily lives of Canadians that is not mentioned. Second, this is a complex set of key parts of daily life. That complexity is defined in a number of ways that have an impact on the capacity of the country to protect each segment from threat:

And what about the safety of those controls?

The following excerpt from the Canadian Energy Pipelines Association is a good example of providing safety assurance of one CI using another that is even more vulnerable to attack: "Pipeline companies monitor their pipelines 24/7 from remote control centres across the country, equipped with sophisticated, computerized sensing and control systems." – www.cepa.com.

- Some contain organizing systems that are large and readily identified, e.g., government, while some are disaggregated and defy clear definition, e.g., food;
- Virtually every boundary of public-private, level of government, and corporate-individual is crossed and re-crossed here; and
- Spatial complexity, a defining characteristic of this large country, adds to the overall intricacy of the situation.

In fact, the way that the *National Strategy* has adapted a sectoral approach to CI definition belies the interrelationships among the sectors. In some cases, there is also the element of mutual dependence. It would therefore be necessary to look at this view of CI as a series of interacting systems, each with its own internal logic but playing in a complex field. For this reason, the federal government attaches particular importance to its cross-sectoral efforts, most notably the Cross-Sector Council.[5]

A third characteristic is that there is little here that is fully Canadian. The north- south integration of the Canadian economy with the United States in the past twenty-five years means that systems vulnerabilities in the United States also come into the picture. That is why efforts at greater planning co-operation with the United States are imperative. For large industry sectors such as energy, CI must be looked at from a North American rather than a purely Canadian perspective. A glaring example of this was the power outage of 2005, when one failure in the United States put all of Ontario in the dark for a number of days.

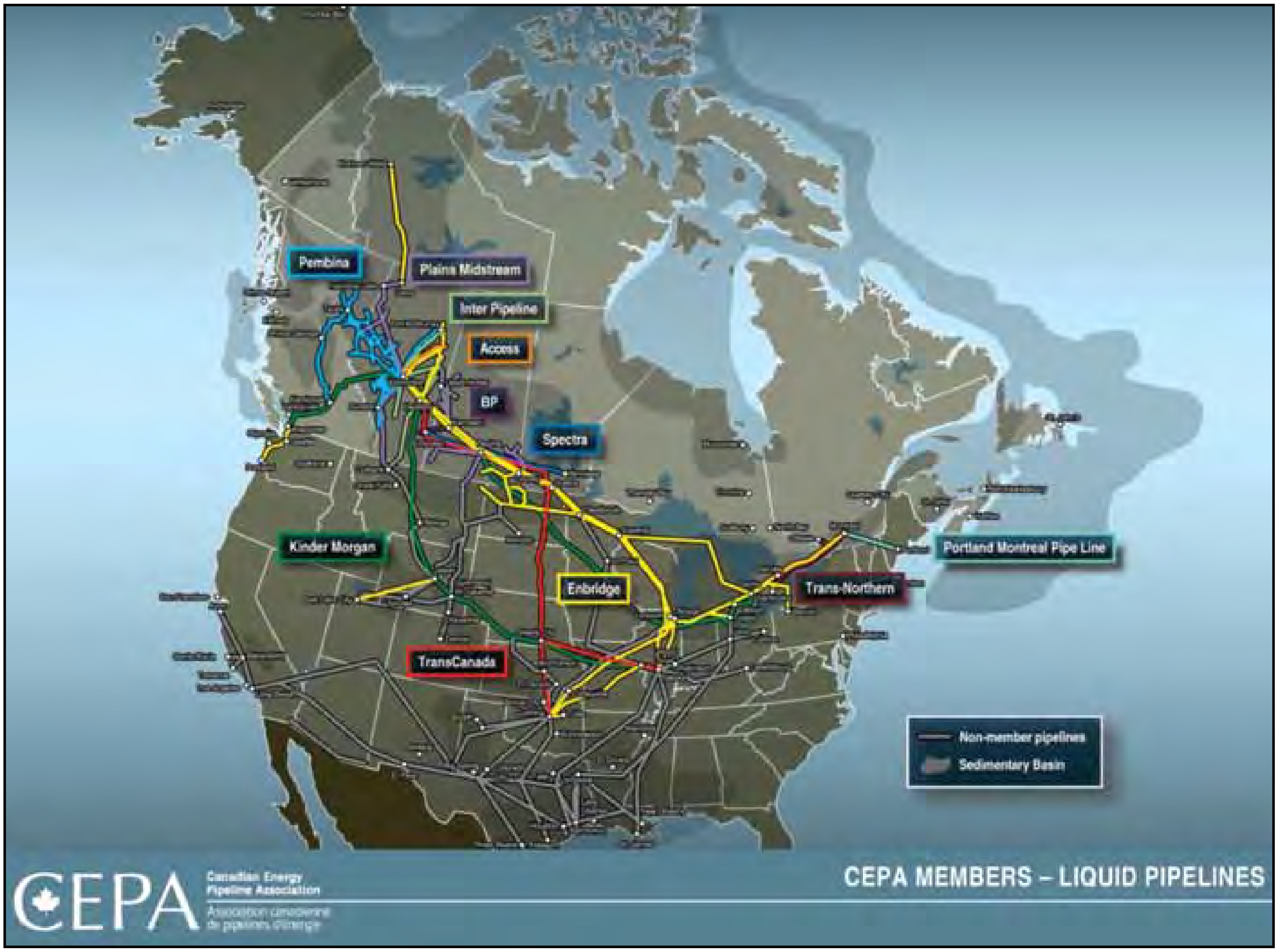
GETTING BEYOND DEFINITIONS

We must give up hope that theoretical frameworks will define CI. Research for this paper and searches along with interview questions cannot determine if, with this framework, we actually know what and where the CI actually is. While the Auditor General of Canada[6] noted in 2009 that some efforts were being made to map CI, there is no evidence that any such mapping has been completed or that if it were it would be used within the sectors or that it would be updated as major investments are made, such as the recent Economic Action Plan, which focused on infrastructure.

In general, the government response is that this "mapping" is up to the sectors to organize their immediate protection plans for assets they own and operate. One example of positive leadership is in the energy sector, in which both major private systems operators and Natural Resources Canada have partnered to map and identify major energy CI for planning purposes.

Further, there is considerable effort in certain sectors, most notably again in the energy sector, to inventory and co-ordinate operations of key assets. For instance, the nearly 100,000 km of oil and gas pipelines in North America are monitored and overseen by regional private sector organizations such as the Canadian Energy Pipeline Association.[7] Similarly, grid-wide electricity standards are set by the North American Electricity Reliability Council, with Canadian membership. It can be presumed that some form of inventory is in place and that there is monitoring based on industry standards, not simply by the individual owners. However, any assumption that a credible linked overview of systems exists is misplaced.

Figure 2: Liquid pipelines of CEPA Members


Pembina
Plains Midstream
Inter Pipeline
Access
BP
Spectra
Kinder Morgan
Enbridge
TransCanada
Trans-Northern
Portland Montreal Pipe Line
Non-member pipelines
Sedimentary Basin
CEPA
Canadian Energy Pipeline Association
Association canadienne de pipelines d'énergie
CEPA MEMBERS – LIQUID PIPELINES

WHO IS RESPONSIBLE?

CI is so widely distributed and pervasive that it is impossible to say who is responsible and who is accountable for CI either as a system or a set of sub-systems. In fact, it can be argued that this is a case of multiple interests crossing all the normal divides of public and private to the degree that there is a real danger that even with titular leadership being lodged with Public Safety Canada, in the end no one is responsible and no one is accountable. In reality, the entire policy process is merely a combination of muddling through and ad hoc problem solving. When faced with an assault on key CI or its breakdown in the face of a natural disaster or total failure due to neglect, the responsibility to prevent, respond, and restore must be clear.

In the end no one is responsible and no one is accountable. The entire policy process is merely a combination of muddling through and ad hoc problem solving.

If ownership is a factor in determining responsibility, then it is important to note that the vast majority of CI is privately owned, although many key elements are publicly owned and operated. There are variations across the country where ownership and the constitutional responsibilities for CI are applied differently. Where provinces have constitutional responsibility, e.g., energy, there are variations in ownership of the assets. In some provinces, these are publicly held. In others, private sector providers operate the systems.

An example of the complexity and crossover quality of responses can be found in Table 1, a 2006 chart of energy disruption scenarios, as part of an evaluation of the energy Infrastructure Protection Division of Natural Resources Canada.

Table 1 Energy Disruption Scenarios

ENERGY DISRUPTION SCENARIO	JURISDICTION	LEAD DEPARTMENT/AGENCY/ COMPANY	ACCOUNTABLE DEPARTMENT/AGENCY
Nuclear Power Plant Disruption	Federal	Canadian Nuclear Safety Comission	NRCan
Conventional Power Plant Disruption	Provincial	Facility Owner	Provincial Departments of Energy
Terrorist Event on Energy Infrastructure	Federal	RCMP / DND/FC	PSEPC
International Border Event (e.g. a pipeline or electrical transmission failure)	Federal	NRCan	NRCan
Natural Disaster (provincial)	Provincial	Facility Owner	Provincial Departments of Energy
Natural Disaster (multi-province)	Federal	PSEPC	NRCan
Multi-critical Infrastructure Failure	Federal	PSEPC	NRCan

Source: http://www.nrcan.gc.ca/evaluation/reprap/2006/e05021-eng.php.

One can only conclude that ownership of CI assets is not on its own the basis for determining responsibility for its protection from intrusion by threat. It does impose upon the owner the responsibility to take reasonable steps given the nature of the threats *as the owner defines them*. However, normal public safety measures such as intelligence and policing also play a role.

To carry out its own responsibilities, the federal government has designated Public Safety Canada as the lead department. However, over 14 other departments and agencies have key responsibilities either in terms of their direct oversight of critical sectors, e.g., Natural Resources Canada and energy or through their pervasive security responsibilities, e.g., Canadian Security Intelligence Service or the RCMP.

BRINGING CIVILIZATION TO ITS KNEES...
Goths
HACK
HACK
HACK
Vandals
HACK
HACK
HACK
Huns
HACK
HACK
Geeks
HACK
HACK
HACK
HACK
KEVIN SIERS ©2000 THE CHARLOTTE OBSERVER

In the view of the federal government, responsibility for CI is widely distributed. In its *National Strategy,* it lists it in the following manner:

> *Responsibilities for critical infrastructure in Canada are shared by federal, provincial and territorial governments, local authorities and critical infrastructure owners and operators – who bear the primary responsibility for protecting their assets and services. Individual Canadians also have a responsibility to be prepared for a disruption and to ensure that they and their families are ready to cope for at least the first 72 hours of an emergency.*[8]

RECOGNIZING A POLICY MASH-UP WHEN WE SEE IT

The issue of responsibility and accountability and the difficulty in answering the fundamental policy questions – Who is responsible? Who is accountable? – highlights the challenge of these issues in the 21st century. CI has to be approached not as an exercise in finger pointing but as a set of complex challenges posed in both policy and operational terms. CI is certainly more of a policy "mash-up" than a simple program focused on a single problem with a single set of readily measured results. A mash-up is a phrase more commonly associated with mixing music for iPods than with complex social and economic policies. However, the analogy is appropriate in this context.

The concept of a policy mash-up is introduced at this point to complement the equally applicable notion of the wicked policy problem defined by its complexity and intractability, often engaging many actors over a long period of time with no clear and easy solution.[9] A policy mash-up is unlike Russell Ackoff's social policy mess: "Every problem interacts with other problems and is therefore part of a set of interrelated problems, a system of problems…. I choose to call such a system a mess."[10] In the 21st century, treating security issues such as CI as being equally complex is almost self-evident. Finding the platforms to resolve such complexity remains a challenge.

The concept of a mash-up suggests that complex problems are increasingly colliding into each other, demanding integrated solutions from various sources. They often reflect the capacity of communities to respond and be resilient in a dynamic environment.

In a traditional conceptualization of even wicked problems, we might think of a lead agency, allocation of specific resources, and fitting the problem into the solution. In a mash-up, we think of the problem first, then the capacity to respond effectively and in a timely way (resilience), then the resources needed no matter where they are, and often bearing down to the individual level.

As the search for responsibility shows, there is no one level of government or CI owner fully responsible for all aspects of the problem. Collaboration is key, something more easily called for than executed. So too is the abandonment of traditional notions of command and control from senior levels of government. This flies in the face of public expectation that someone is in control of policy and can be held to account for policy successes and failures

It is probably for this reason that Public Safety Canada emphasizes its role in bringing the various players together. In truth, it can do very little. It focuses on risk assessment tools, sharing information, and the creation of sectoral councils. At the first meeting in December 2010 of the Cross-Sector Forum, an umbrella group, the following goals were set:

1. Develop common understanding of what CI is;
2. Create a framework for sharing sensitive information;
3. Identify of key assets and systems; and
4. Identify key vulnerabilities.[11]

What is striking about this list of objectives is that it shows Canada at a fairly preliminary stage in CI planning: gathering information and developing common definitions.

Canada is at a fairly preliminary stage in CI planning: gathering information and developing common definitions.

Further evidence of the mash-up nature of CI protection is the instructive tale of Hydro One's Niagara Reinforcement Project and the protracted standoff in the Caledonia aboriginal lands in Ontario. This project, designed many years ago and with all the regulatory approvals in place, was slated to upgrade transmission line safety in the Niagara Region, while also impacting CI stability for Hamilton and the Greater Toronto area, a prudent part of building CI resilience. However, the $116 million upgrade, originally slated for completion in 2007, remains stalled due to the land claim dispute that continues to simmer in Caledonia. This is an example of how CI upgrades and hence long-term sustainability are threatened directly by militant resistance, but also, some would argue, by public policy in that the Government of Ontario is reluctant to confront this resistance.[12]

WHAT IS THE THREAT?

The objective is a national critical infrastructure that functions well within anticipated parameters, where disruptions are responded to in a resilient fashion and where the active potential for unanticipated disruption is assessed through rigorous risk management. Thus, threats to CI must be seen as a broad spectrum that does not simply start and stop with current, top-of-mind issues such as terrorism and natural disasters, but extends into such matters as public policy, due diligence by private firms, and increasingly, adequate investment in maintaining a healthy and resilient CI inventory. Further, one cannot discuss threats in isolation. There are many threats in the world – and a few outside it such as asteroids on their way to Earth. On cannot realistically accommodate all possible threats. Layered into the discussion, therefore, must also be the notion of risk: How likely is this threat to actually happen, and how severe would the impact be? Finally, the concept of vulnerabilities must be added to the mix. How vulnerable is the system or sub-system?

Your threat is someone's opportunity

It pays in developing an appraisal of threats to undertake alternative forms of analysis, such as ones that take the perspective of the possible threat agent. One technique is known as *red teaming*, a practice of viewing a problem from the perpetrator's perspective. This forces organizations to answer tough and often glossed-over problems they may have with CI vulnerability.

See Warren Fishbein and Gregory Trevetnon. 2002. "Rethinking Alternative Analysis to Address Transnational Threats." Sherman Kent Center for Intelligence Analysis, Occasional paper: Vol. 3, No. 2.

Threats to Canadian CI have proven more latent than real, especially from human sources. While the targets are obvious, especially in the energy sector with its extensive distribution and transmission systems and vulnerability along long distances, little has taken place in terms of such threats. That does not mean that there have not been attacks by people. Some have been persistent but local, such as the attacks on pipelines in north-eastern British Columbia in 2007-2009. It has to be noted that the RCMP quickly labelled this series of six attacks "domestic terrorism"[13] without providing much guidance to the public about what that meant. Without discounting the seriousness of these attacks, they illustrate the challenge facing both the public and private sectors in defining the nature and source of CI threats. Is this series of attacks terrorism, with all that implies as an attack on society in general and the established order, or is it, as Paul Joosse of the University of Alberta suggests, a more localized event that borders on vandalism?[14] Seeing threats to CI only through the lens of terrorism minimizes what is probably a series of more pressing and real threats. For example, systematic attempts at theft of vital components of CI must be treated in the same way that an individual terrorist act would be. The outcome is the same when copper wire is stripped out of a large, poorly protected transmission node whether it is stolen by an organized crime group for resale or destroyed to incapacitate a large city.

Canada is vulnerable to attacks on energy infrastructure aimed at disrupting service to the United States.

Natural disasters and the failure to maintain infrastructure adequately represent, on the face of it, greater threats. But Canadians must take a longer view of these critical assets, for they figure significantly in our relationship with our largest trading partner, the United States. Indeed, as a 2006 Conference Board of Canada report points out, the concerns we have for threats must be tied directly to American dependence on Canada a supplier of reliable multiple energy sources.[15] As Jacques Shore points out in his 2008 paper for the Carleton Centre of Intelligence and Security Studies, "Canada is vulnerable to attacks on energy infrastructure aimed at disrupting service to the United States."[16] What we have also discovered is that attacks on American CI can incapacitate Canadians.

Two key questions guide the discussion of threats to CI: How vulnerable are we? How much safety can we afford? However, when thinking about CI in a systematic fashion, it is important to define threats carefully. One should not be guided exclusively by the simple agency view of threats: there is a person out there intent upon harm to some element of CI, with the opportunity to act and the capability to perform. Further, the specific CI component may simply be a limited target aimed at higher purposes, e.g., political destabilization, terrorizing a population to induce a loss of freedoms, or personal gain. This agency notion of active threats is certainly valid, but it is incomplete when thinking about threats to CI in a comprehensive, all-hazards approach.

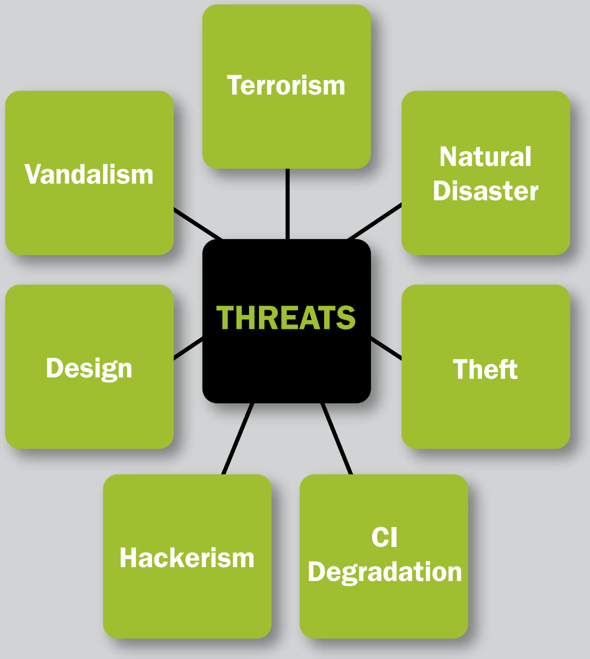
ALL-HAZARDS APPROACH TO THREATS

Develop all-hazards risk analyses that take into account accidental, intentional and natural hazards.

All-hazards is a term coming into common use when assessing threats. In fact, the *National Strategy* adopted it as the core approach to analyzing threats to CI. It states, "Federal, provincial and territorial governments will collaborate with their critical infrastructure partners to develop all-hazards risk analyses that take into account accidental, intentional and natural hazards."[17] It does not define what it means by an all-hazards approach, implicitly taking the view that everyone will know what it means.

An all-hazard approach entails developing and implementing appropriate responses for the full range of likely risks and emergencies: natural, biological, technological, and societal. An explicit part of this approach is that CI protection and resilience is not simply associated with terrorism. This has certainly been born out over a series of CI failures in the past decade. In fact, terrorism has played a relatively small role in CI incidents over that period. A further benefit of the all-hazards approach is that it recognizes that risks and vulnerabilities to systems can be used by those with terrorist goals: terrorists attack the weak systems.

Figure 3: Threats to CI



An all-hazards approach recognizes that risks and threats can come from more than just active agents. It recognizes the role of natural disasters and accidents as risks. However, what it does not do is apply core principles of risk analysis that define which hazards are important and which are not. Further, an accurate assessment of the degree of risk or hazard needs to overlay onto the identification. In having an all-hazards approach, one has to avoid excessive analysis of the cost of measured and targeted responses. This is a tough balancing act that requires the avoidance of groupthink and the rejection of bad news. One has to avoid the "this could never happen here syndrome" but also what Dan Gardner[18] identifies as the available heuristic, which would suggest that if a threat or risk is real somewhere else, it is also real and present in Canada.

Threats are about sources of disruption. Risks are about consequences. Figure 3 outlines the threat landscape that can be applied to CI in Canada.

TERRORISM

As has been pointed out already, much of the thinking about CI protection and resilience at the national level has focused on terrorism. The at hand definition of terrorism, however, deserves some examination. Terrorism has to be seen not only from the global perspective but also from the domestic. It is therefore any organized, no matter how transitional, group that wants to use CI disruption or destruction to achieve broader ideological ends. In Canada, we have seen few direct attacks from international groups, even though some have clearly identified Canadian CI as a good target. However, we have seen the disruption of rail and highway activity through Mohawk territory in Ontario a number of times in the past decades. While these actions were brief, they were, nonetheless, an effective attack on vulnerable CI. Were these acts terrorism, insurgency, or merely a reasonable political protest?

Much of the thinking about CI protection and resilience at the national level has focused on terrorism.

Another aspect of the terrorist threat to CI is the way in which the target is chosen. The 2007 study, *Assessing Terrorist Motivations for Attacking Critical Infrastructure* by the Center for Nonproliferation Studies in California offers the following insight:

> *CI [Target] Characteristics are among the most important factors in a terrorist group's decision to attack – or not attack – specific targets. The most important characteristics of an infrastructure target that tend to affect terrorist targeting are its: 1) level of protection; 2) whether or not it has a high profile (which is in part a function of how much attention the media has paid to it); and 3) its actual function. All [other] things being equal, terrorists are more likely to select targets that are vulnerable. At the same time, they wish to attack functionally important, high-profile targets, the damage or destruction of which will be costly to society. The key decision-making factor is usually the relationship between a facility's vulnerability and its desirability as a target. Given the large number and wide range of potential targets, terrorists will tend to avoid heavily-fortified or heavily-protected targets, unless these have extraordinary significance, and instead attack more vulnerable targets.*[19]

In the context of radical First Nations groups intent on major disruption, the logic is impeccable. As Shawn Brant, one of the leaders of the Mohawk blockade said two hours after they dismantled the railway barrier: "Believe it or not, this is the first soft step of the campaign… We have identified three different targets [the railway, provincial highways, and the town of Deseronto] and will escalate the degree of severity necessary."[20]

The point to be made here is not that legitimate civil protest is terrorism or undesirable. The line between protest and the ideological targeting of CI is one that crosses into criminal activity. We have to recognize that in Canada, both global and local sources of terrorism are possible. Other sources of domestic terrorism can be environmental, anti-abortion, animal rights, anti-globalization, and white supremacy groups.

The other sources of terrorist activity that could affect CI is based on Canada's proximity to the United States and the fact we are home to a diverse array of ethnic groups, some of whom have small elements engaged in homeland conflicts off Canadian soil.

By far the greatest threats to Canada's CI are natural disasters. Natural disasters have accounted for 69.9 percent of all disasters in Canadian history.

NATURAL DISASTERS

By far the greatest threats to Canada's CI are natural disasters. While the built CI environment takes storms, floods, and related threats into account in design, extreme circumstances can quickly and decisively shut down major parts of the country. A 2003 Public Safety Canada document, *Threats to Canada's Critical Infrastructure*, points out the following:

> *According to the Canadian Disaster database, natural disasters have accounted for 69.9 percent of all disasters in Canadian history. Flooding has been, by far, the*

> *greatest cause of disasters in Canada in the 20th century, followed by severe storms. Although natural disasters are necessarily prompted by a severe natural phenomenon, it must be iterated that human impact on the environment can play a significant role in both the prevalence and scope of certain natural disasters.*[21]

Not all threats involve acts of deliberate sabotage. Some involve neglect, whether benign or deliberate.

THEFT

Hydro One identifies the theft of its assets, most notably by organized crime groups, as the most pressing threat it faces on a regular basis.[22] Occasional theft is one thing. The systematic effort to remove valuable assets without regard for the consequent functionality of the system is a much greater threat.[23] Similarly, threats of disabling large portions of Internet connectivity or applying masking software to enable the removal of financial assets is a primary preoccupation of the banking industry.

The other element of the theft threat is that of insider theft. These are employees abusing their privileged access to internal systems, information, and assets for personal gain. This problem exists in many non-critical industries as well, especially where attractive asset items can be removed and controls are less than effective or can be masked. For a CI asset, such threats can compromise the CI capacity and resilience, especially if carried out in a systematic and long-term fashion.

CI DEGRADATION

Not all threats involve acts of deliberate sabotage. Some involve neglect, whether benign or deliberate. Such neglect can manifest itself in the failure to maintain CI assets adequately, the failure to replace it in a timely fashion, failures in controlled part assessment, or budget cutting that increases the risk of failure. This can happen in the public and the private sectors.

DESIGN

CI design can leave it open to a greater level of threat than other possibilities. Further, some design elements such as how to cover great distances with low populations over rough terrain will leave the CI more vulnerable *by design* for reasons of cost, lack or realistic alternatives, or simple geographic imperatives. As John Robb of Global Guerrillas pointed out in 2004, "Complex systems, like the Internet, operate well beyond the influence of any central management group and the thinking of the original designers. This research shows that the core design and operational decisions made by these groups does have a major impact on the ability of the system to respond to damage."[24]

HACKERISM AND VANDALISM

It could be argued that hackers are just cyber-vandals, and there is some truth to that. However, it is worth noting how often CI is subject to random attack with no intent other than to mess things up. Hackerism is singled out as it is a relatively new form of vandalism. Further, there is likely little personal gain, except for the psychological rush of penetrating into control systems in major CI assets.

Both these forms of more random threat can come from outside or inside sources. One of the reasons that CI assets are so vulnerable to insider attack is the unique knowledge that insiders in many CI sectors possess. Whether they are nuclear scientists, engineers, medical specialists, or food scientists, they are specialists in their fields, but also possess knowledge of the information and infrastructure pathways of the CI asset in which they are working. A 2008 study on insider threats to CI pointed out how little is known of this phenomenon. CI asset owners tend to treat this internally, avoiding publicity where they can. They fear loss of confidence in their business as a result. Hence, little is known about insider attacks.[25] The study further points out that even the concept of the insider is changing with globalization: "The dynamics discussion identifies that rapidly escalating technology and network risks are combining with growing globalization of workforces, supply chains, and service providers to produce new threats and risks."[26]

- Moving from holding customer billing information to full customer profiling information, including geographical layers of analysis;
- A change from heterogeneous technology to standardized and homogeneous technology with greater connectivity to external systems; and
- A shift from traditional service modes to on-line business and e-commerce in both the public and private sectors.[27]

All the above create greater IT dependence. They also create greater vulnerability to interference not just in using computers as a communications tool, but using IT to access directly personal information and wealth and to interfere with the smooth operations of CI to the point of shutting it down or masking attacks on it.

Canada's level of threat is directly linked to that of the United States.

SHIFTING GROUNDS OF CYBER INFRASTRUCTURE

With all the talk of cyber-threats, it is reasonable to consider that there are multiple threats coming from this area. In fact, these threats cross most of the sectors and create new and emerging vulnerabilities not just to computer systems, but also to the actual operations. Over the past two decades, dramatic shifts have taken place in the way many elements of CI operate. Nancy Wong of the US Critical Infrastructure Assurance Office noted the key elements of this shift:

- A movement from human operated facilities to automated ones;
- A change from remote human monitoring to automated remote monitoring and control;
- A shift in focus from local markets to open and globalized markets;
- Moving from local customer services to consolidated call centres;

THE CURRENT LEVEL OF THREAT

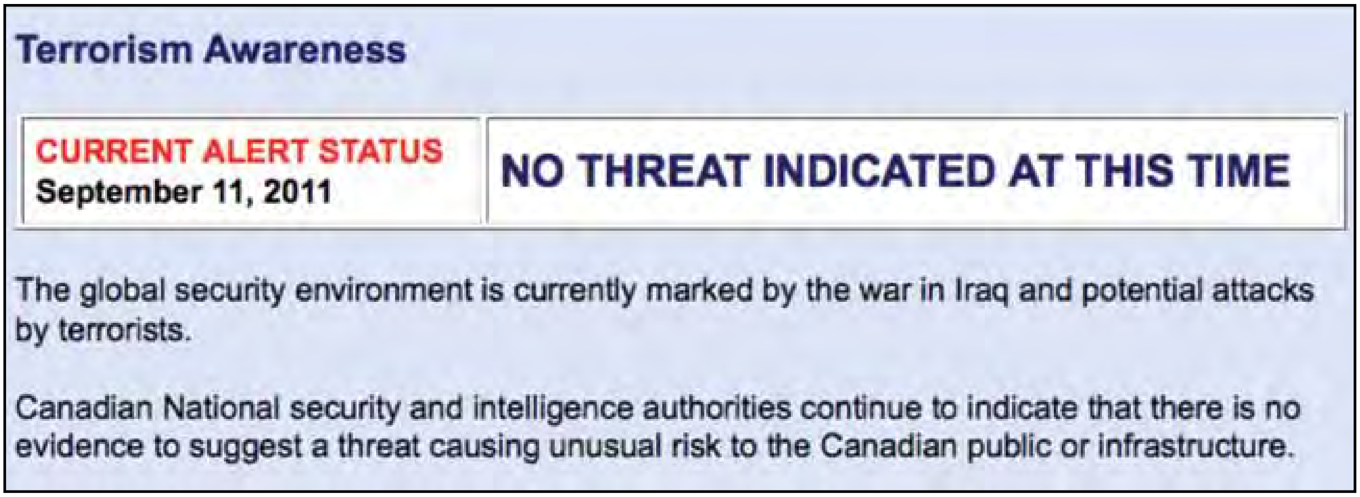
It is impossible to provide a simple view of the threat level to Canada's CI. It is too complex and distributed to do that. While there is much information flowing through both public and private systems, it is not aggregated into a simple view and probably cannot be. That does not mean that more effort is not needed to develop vulnerability maps. However, they will not translate into sound bites. Further, the threat level is also in the eye of the beholder or exaggerated by special interests. Some factors are real and, regardless of any immediate emerging threats, have to be part of a continuous perspective on threats to CI:

- Canada's level of threat is directly linked to that of the United States, both in real and perceived terms.
- Governments are reluctant, quite rightly, to issue global threat alerts that frighten the population or lead to no consequences but expenses to private firms.

- Frequent alerts or too much information produce alert fatigue and desensitize responses.

- The highest level of threat to Canada's CI rests in the areas of natural disasters and system degradation, both of which lend themselves to investment in resilience and redundancy.

Figure 4: Sample Threat Level Notification



Terrorism Awareness

CURRENT ALERT STATUS
September 11, 2011

NO THREAT INDICATED AT THIS TIME

The global security environment is currently marked by the war in Iraq and potential attacks by terrorists.

Canadian National security and intelligence authorities continue to indicate that there is no evidence to suggest a threat causing unusual risk to the Canadian public or infrastructure.

Source: British Columbia Emergency Preparedness Advisory System, September 11, 2011

One has to take the overall threat level to Canada's CI seriously. However, the only way that the risk posed by those threats can be assessed is through specific case-by-case analysis. Risks add the dimensions of probability and severity to threat analysis, key variables in determining how scarce prevention resources should be distributed. The vulnerability of Canada's CI does have some important defining features that, while not unique, certainly are distinct: sparse population, distributed in a small number of large, widely separated urban areas, long supply lines often running through areas with little support or security infrastructure, increasingly monitored by remote control systems to reduce costs. Evidence suggests that both the government and the private sector understand these inherent vulnerability characteristics and take the matter seriously. The challenge is how to develop a useful and realistic appreciation of the current risks within that context.

The highest level of threat to Canada's CI rests in the areas of natural disasters and system degradation.

One also has to consider resilience within current systems. To date, Canadian CI has proven resilient in the face of infrastructure threats. While these have mostly been natural disasters, one can also point to the successful police actions in Toronto/Brampton against a domestic terrorist threat as a demonstration of the relative strength of current systems. While that resilience is there, two vulnerabilities are also present. The first is the increasing interdependence of CI systems and sub-systems with those of the United States, which could lead to attacks intended for the United States taking place in Canada. The second is the speed with which cyber security issues are emerging, not just within the Internet and attacks on computer systems, but the use of those tools to disable key CI.

From the Public Safety Canada website

"The Daily Infrastructure Report has been decommissioned effective July 15, 2011 and will no longer be produced and disseminated."

http://www.publicsafety.gc.ca/dir/index-eng.aspx

GOVERNMENT RESPONSE

In the heady days after the 2001 tragedies, the federal government asserted a leadership role in protecting CI in Canada. What has emerged over the past 10 years, however, would appear to be little real progress beyond setting up communications and supports in this complex field. Seen from the outside, the efforts over that period had a stop-start quality, with more plans to plan than actual changes or results. In 2002, the federal government announced the National Critical Infrastructure Assurance Program (NCIAP).[28] In 2004, it produced *Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection.*[29] In 2005, it began a series of consultations with other levels of government and industry stakeholders. This process of consultation, while issuing a series of broad policy statements, led to little clear action. That being said, certain sectors such as energy acted promptly within the confines of the existing regulatory systems. For instance, in the nuclear field, the Canadian Nuclear Safety Commission acted in 2006 to tighten security requirements for nuclear plants. Many instances of this sort of action can be found within specific targeted sectors.

Reflecting the reality that CI in Canada is linked to the United States, in 2011 the two governments signed the Canada-United States Action Plan on Critical Infrastructure.

What cannot be found is a consistent pattern of overall government action and co-ordination. In fact, once the 2005 consultation round was complete, the federal government in essence reissued its policy framework, under new leadership from the new government, but with many of the attributes one can find right from the beginning: planning, co-ordination, and communication. In fact, in 2005 the Auditor General of Canada said the following about the statement of emergency preparedness:

> *In many cases, spending on emergency preparedness was not guided by a thorough analysis of threats and risks; as a result, funds to strengthen emergency response capacities have been poorly allocated. For example, the opportunity was not taken to create a national pool of equipment that is compatible and interoperable.*[30]

Much has been done in this area since that time, a fact later acknowledged by the Auditor General.

The promised federal policy on Critical Infrastructure Protection, envisaged in 2004 and arising from the consultative process was finally delivered in May 2008. In seeing some time elapse one may have expected a major shift aligning with the many events and responses that had taken place in the interval. In fact, the policy reiterated the coordinative, consultative, and communications leadership role of the federal government. The policy led to the creation of the *National Strategy for Critical Infrastructure*, followed by the *Action Plan for Critical Infrastructure*.

In essence, the objectives of this strategy and action plan are:

- To build trusted and sustainable partnerships through creation of a National Cross-Sector Forum to improve communications;
- To implement an all-hazards risk management approach by risk assessments of Canada's critical infrastructure at federal, provincial, territorial, and sectoral levels;
- Public Safety Canada will coordinate this in cooperation with sector networks, key federal departments and agencies, provinces, territories, and the private sector;
- Develop emergency programs and plans through collaboration between lead federal departments and agencies for each sector, province, and territory, and the private sector;
- Conduct exercises and assist in the coordination of regional exercise planning across jurisdictions and with the private sector;
- Advance the timely sharing and protection of information among partners by a wider range of information products (e.g., risk assessments, incident reports, best practices, lessons learned, assessment tools);
- Improved delivery mechanisms (e.g., web-based critical infrastructure information);

- Improved protection of shared information from unauthorized disclosure; and
- Expanded production of all-hazards risk information products.[31]

Reflecting the reality that CI in Canada is linked to the United States and that many of the threats on Canadian territory are really aimed at the United States, in 2011 the two governments signed the Canada-United States Action Plan on Critical Infrastructure.[32] While calling for greater co-operation and communication, it recognized the mutual dependencies that had developed in this area. It also further aligned the federal approach of consultation, communication, and partnering with a similar orientation in the United States. The objective of the Agreement is to recognize:

> *The interconnected nature of critical infrastructure requires a coordinated Canada-U.S. approach; regional approaches to cross-border collaboration need to be guided by an overarching Canada-U.S. framework for critical infrastructure; strong private sector collaboration across the border needs to be supported with an integrated Canada-U.S. approach; uncoordinated efforts increase the likelihood of wasteful duplication of efforts that can be managed through collaborative development and sharing of best practices; and communications with critical infrastructure stakeholders (both domestic and cross-border) need to be coordinated, accurate and timely.*

The private sector is vulnerable in the efficiency of its internal sharing of information.

It is of interest to note the recognition of the regional nature of the CI challenge. While much of the flow of issues is north-south, individual regions face unique challenges across the continent. This is an issue that has been highlighted by the Conference Board of Canada. As it pointed out in its 2011 report, *Regional, Cross-Border Planning: Maine-New Brunswick Action Plan for Infrastructure Protection and Resilience*, "the growing list of national and bi-national statements of critical infrastructure protection and resilience has set significant objectives that will require a regional component in order to be successful."[33]

The Action Plan arising from this Agreement bears remarkable resemblance to the Canadian Action Plan, but adds the international, north-south complication:

- Seek direction from the Canada-US working group on critical infrastructure;
- Develop compatible mechanisms and protocols to protect and share sensitive critical infrastructure information;
- Identify public and private sector information requirements to support the development of valuable analytic products tailored to their respective and unique decision-making, protection, and resiliency requirements;
- Collaborate to ensure effective information sharing during and following an incident affecting critical infrastructure;
- Establish a Canada-US virtual infrastructure cell to develop and share risk management tools and information;
- Assess risks and develop plans to address priority areas and measure the effectiveness of the plans in reducing risks to the United States and Canada; and
- Provide mechanisms and opportunities for the US Sector and Government Coordinating Councils and the Canadian sector networks to work together to improve sector-specific cross-border collaboration.

The core question has to be asked: does all of this activity with its array of committees, communications, and sharing of information actually constitute action? Dr. Martin Rudner, founding Director of the Canadian Centre of Intelligence and Security Studies, has described this approach as essentially defensive.[34] Jacques Shore has described it as state-centric.[35] On the other hand, Kevin Quigley of Dalhousie University and author of *Responding to Crises in the Modern Infrastructure* has described this public policy challenge as "mind boggling and complex".[36] While these efforts to build stronger ties are commendable and probably absolutely necessary, they are hardly the desired end state. What that state might look like remains unarticulated.

INDUSTRY RESPONSES

Any discussion of CI protection has to recognize that the vast majority of CI holdings are privately owned. While government regulation plays important roles in virtually all involved sectors, the degree of intervention varies. Further, from a national security perspective, the sources of CI disruption from a private perspective can often be different than that of public officials. While there is a strong tendency in public documentation and interviews to go quickly to agency threats, e.g., terrorism or intentional attack, the predominating preoccupation of most private sector CI owners would appear to be unintended damage to assets and aging infrastructure. Further, what some private CI owners are also facing are the consequences of infrastructure failure, such as pipeline leaks, that present major challenges in terms of potential damage to the environment, their reputation, and their bottom line.

What is important in trying to marry private and public interests is that there has to be active recognition that there are different perspectives and orientations, but that the issue of CI safety does indeed cover the range of potential failures. The consequences for the Canadian public remain the same. It is seldom the case that private industry identifies terrorism as a prime concern. Interviews reveal a concern for theft, vandalism, and unintended damage to CI assets. Philippe Reicher of the Canadian Energy Pipeline Association pointed out that external damage to pipelines is the greatest level of concern for the overall system. This is caused, however, mostly by activity near the asset such as digging in construction sites. He writes, "external interference was the cause of six failure incidents and 40 damage incidents on CEPA pipelines during the period 2002-2009. All CEPA external interference failures during the period 2002-2009 were caused by third parties."[37] However, it is clear that the third parties referenced would fit into the category of the general public and not agents with specific criminal intent.

There is a divide between the public sector with its focus on large-scale terrorist activities and pervasive natural disasters, and the private sector with a more specifically focused agenda.

Most industries operating within the CI framework have developed security alert systems of their own. Most notably within the energy sector, security and infrastructure are important and mechanisms are in place for sharing information. The industry does not rely upon government at the operational level for its information. Rather it relies upon more localized police services based on established protocols. Governments would be wise to use these hard-wired mechanisms rather than creating new ones. The private sector is vulnerable in the efficiency of its internal sharing of information.

SITUATION ANALYSIS

Forming a holistic view of the relative state of CI protection is difficult. The situation is dynamic, subject to forces beyond human control.

However, some issues persist within the realm of the possible. These include:

- Getting information sharing right – both a cultural and technical challenge;
- Getting infrastructure investment on an orderly footing;
- Watching the right stuff, i.e., adaptable intelligence about threats, risks, and vulnerabilities; and
- Increasingly, ensuring the presence of well-trained, well-informed, and connected professionals operating sub-systems and working with others in similar situations to increase overall system reliability.

PERSPECTIVE AND THE FLOW OF INFORMATION

There appears to be a divide between the public sector with its focus on large-scale terrorist activities and pervasive natural disasters, and the private sector with a more specifically focused agenda. Further, within government there is a divide regarding focus on concerns between the front-end operational organizations such as the field operations of the RCMP and its own headquarters. In addition, the private sector and operational government units will minimize international threats and focus on the local while the integrative efforts of Public Safety Canada will tend toward generalization of threats. Bridging this divide is a challenge. Neither perspective is wrong and each must, in turn, be given its respectful role. It does present a challenge when resources are scarce, especially the resources of time and attention.

Industry has proven reluctant to provide information to the federal government until it is convinced that protections exist.

An example of this inertia was the establishment by the RCMP of its Suspicious Incident Reporting (SIR) system. Launched in 2008 on a pilot basis, it was established by the National Security Criminal Investigations unit to provide a clearinghouse on reports of information on suspicious incidents. It is purely voluntary. For large private CI assets managers, this can be a valuable source of information. The challenge that this new utility has posed for private CI asset holders is that it circumvented the established local police connections vital to the identification of specific threats. It was a national reporting system, another piece of the information puzzle, and not fully integrated into street-level policing. These are early days for such a service and lessons will certainly be learned. It is also unclear about how the information, once gathered, is distributed even within the diverse RCMP organizational structure.

With respect to information sharing, industry has proven reluctant to provide information to the federal government until it is convinced that appropriate protection mechanisms are in place. Access to Information and Privacy (ATIP) legislation is a concern. Even with the federal government's efforts to provide exclusions and protections of the information, there remains a cultural reluctance to share information. This is a major challenge for the government that will only be resolved with long-term stable relationships that build trust.

In 2006, the federal government created the Centre for Security Science to develop research capacity in a variety of security areas. CI is one of its key lines of inquiry. It works with academic institutions and private sector firms and associations on a range of research projects, disseminating the findings through its website, separate publications, and symposia. The CI component is managed by the Public Security Technical Program.[38] An examination of the research produced stresses the specific nature of most of the work being undertaken. These are practical applications covering the range of concerns of the 10 sectors identified as part of the CI portfolio.

Figure 4: Control Panel at Nuclear Plant – Control Threats

Source: http://abcnews.go.com/Politics/nations-infrastructure-vulnerable-cyber-attack/story?id=14225674

Are threats to CI being given the attention and resources they deserve? Clearly government is trying to respond with various efforts at communications and research. The challenge is that no one has been able to calibrate when enough is enough. We are in the zone of the "black swan"[39] of risk – the low-probability, high-impact event. This zone, especially as it applies to CI, demands the capacity for well-trained reliable professionals to have sufficient redundancy in the system for adaptive response.

MANAGING THE MASH-UP: GOING FORWARD

To begin to piece together the agencies, governments, and private companies that are involved in CI use and protection would require more research than this monograph permits. In addition, a new forest of acronyms is arising in what is clearly an expanding field or growth business, including CCIRC (Canadian Cyber Incident Response Centre) and ITAC (Integrated Threat Assessment Centre).

To say that Canada has its act together with respect to critical infrastructure threat, protection, and response capacity would be a stretch and somewhat misleading. However, many developments are underway that, if taken together, would both identify and mitigate risks in a more integrated way. That being said, the challenges are daunting. No clear path exists to sort out responsibilities and accountabilities, who will pay, and how to bring less than willing partners to the table. As Robert Dick, Director General of the National Cyber Security at Public Safety Canada said in a recent interview in *Vanguard Magazine:*

To say that Canada has its act together on threats to infrastructure, and proper protection and responses would be misleading.

> *It is incredibly complex. We've made these information systems so integrated and prevalent in our lifestyle and in the way in which government and the economy operates. Cyberspace is a pretty fluid environment and things evolve rapidly, so the complexity derives from how all encompassing this strategy is and the fact that no one actor can do it all. It really was a matter of unravelling a bit of that complexity, figuring out the different elements and what everybody has to do in a federated environment where 85 percent of critical infrastructure is owned or operated outside the federal domain and where responsibility for many issues lies in the jurisdictions of the provinces and territories, including regulating much of Canada's critical infrastructure. That requires a lot more sharing and collaboration than perhaps we've been doing in this space.*[40]

The federal government is placing a lot of emphasis on its role in bringing parties together. It points to the creation of the Cross-Sector Forum, which held its inaugural meeting in December 2010, as a key integrator. This Forum identified four priorities:

1. To develop a common understanding of what CI is,
2. To develop a framework for sharing sensitive information,
3 To identify key assets and systems, and
4. To identify key vulnerabilities. [41]

While these priorities are laudable, questions have to be asked: What has been going on in the 10 years since 9/11? Who is to be held to account for years of inaction that may have endangered Canadians? No clear answers exist. Given other government activities, however, it is intuitively clear that much has been done. It has not been pulled together in the way that the cross-sectoral approach would aspire to do. The real test will be to determine if this high level form of co-operation, built around a hierarchy of relationships rather than a network, is the most effective means to achieve the desired results: timely sharing of relevant information on risk and threat without overloading systems, creating panic, or adding unwarranted costs.

It is not as if the threats are clearly known. In some cases they are evolving rapidly. For instance, cyber threats cross traditional functional boundary thinking that pervades the early CI approach – energy, water, food, etc. Given how rapidly some of these sectors are becoming integrated and relying on distant centralized computer control and monitoring systems, the cyber threat is a meta-threat, crossing and enlarging the field of vulnerability. This can be scary stuff, but it can also be dramatized and exaggerated to the advantage of particular groups. Governments cannot chase ghosts without endangering their own credibility and creating unnecessary panic.

GOING FORWARD: IS THIS AS GOOD AS IT GETS?

Given the dispersed nature of CI itself and the number of players public and private, is the current state of CI protection adequate? Two responses flow out of this analysis. First, it is never enough. This is a dynamic field, one in which situations change quickly, new intelligence arises, new technologies come into play, and vulnerabilities and risks evolve. Therefore, no one with any responsibility for either specific CI components or the oversight of the total system has the right to declare that their efforts are sufficient. The objectives outlined below therefore stress the need to support this dynamic system of information exchange, investment, and public awareness. Second, governments need to step up to the plate in their leadership roles, moving beyond communications to building and operating systems of communication and problem-solving that are interoperable and avoid unsupported cost transfers to each other or the private sector. They need to be more systematic in mapping CI, in documenting inherent vulnerabilities and emerging risks, and more explicit in funding infrastructure renewal to ensure that they do not create more vulnerabilities by permitting CI to degenerate. Just getting people talking is a start, not an end.

Governments need to step up to the plate in their leadership roles, moving beyond communications to building and operating systems of communication and problem-solving.

What appears missing in the research interviews undertaken for this paper is a sense of a desirable end state that addresses the safety of the infrastructure itself. That is a tough aspiration. No one can provide global and permanent assurance. That would be foolhardy. What one can provide is a sense of the true vulnerabilities, threats, and risks on a systemic basis, grounded in the reality of the various sub-elements of CI. To date, we have not seen that information provided to the public in a way that gives assurance that there is a coherent effort to adequately manage the dynamic system, or that the true issues are being addressed, not those dramatic but unreal threats that attract less informed and sensationalized attention.

What then should be the objectives of a resilient CI protection strategy? Surely the over-riding objective has to be a robust and dynamic system, well established, funded, and sustained, that ensures an understanding of the threats, risks, and vulnerabilities to CI as it is known and documented, that can respond to changing circumstances, that meets the needs of public safety, system sustainability, and full disclosure, and that is sufficiently robust to adapt to changing circumstances quickly. A sub-objective is to have a level of public and private support to the sustaining of CI to avoid increasing the vulnerability of CI through deterioration.

Some of the key elements needed to meet this objective are:

- A clear mapping of CI in the country;
- A common understanding of the threats and risks that drive mitigation in both the public and private sector;
- Effective intelligence, 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 contain alarmist or ill-informed fears and misunderstandings;

Ways to provide incentives for the private sector to invest in CI protection without taking on the burden themselves. This could include some form of tax incentives, depreciation privileges, or cost write off; and

Understanding that the human dimension has to be addressed in that systems can only work reliably when the personnel are equipped with the requisite skills, information and tools to hold them together. As Schulman points out, the professional skills of systems operators are typically ignored in system designs, thereby failing to factor in investment costs in them.

Governments need to provide incentives for the private sector to invest in CI protection.

BEYOND COMMAND AND CONTROL: BUILDING A CULTURE OF MINDFULNESS

What strikes one about the issue of CI protection is how organic it must be in order to be effective. Command and control systems will not work to ensure that all the players need to provide a resilient system is created and sustained. It is incumbent on national leadership to take an inclusive approach as Andrew Archibald and Gilles Rhéaume point out in their report for The Conference Board of Canada:

> *Knowing that much of society is dependent on critical infrastructures, it simply makes sense to include the owners and operators of these infrastructures in preparation, training, and exercises. In most incidents, such as natural disasters and terrorist attacks, critical infrastructures are disrupted and victims lack access to essential goods and services. Knowing the capabilities and assets of the private sector prior to incidents can help the public sector ensure effective deployment of all available resources during the response and recovery.*[42]

That being said, there is also considerable thought put into ensuring that no system can provide absolute protection – returning to the titular theme of this paper: when is safe enough safe enough? In 2006, the Critical Infrastructure Task Force of the Homeland Security Advisory Council concluded, "Policies and strategies focusing on achieving resilience would be more robust than current guidance, which focuses primarily on protection."[43]

The Task Force saw the protection strategy as leading to a dead end: "Protection, in isolation, is a brittle strategy. We cannot protect every potential target against every conceivable attack; we will never eliminate all vulnerabilities. Furthermore, it is virtually impossible to define a desired end-state – to quantify how much protection is enough – when the goal is to reduce vulnerabilities. It is extremely difficult to build a business case for protection as a purely defensive strategy. This is due in part to the "How much is enough?" dilemma, and, in part, because businesses typically do not own or control all of the resources on which they depend, and therefore have limited ability to protect those resources."

Both these comments point to the need for all those involved in CI protection to build their organization's awareness of threats in a way that facilitates realistic assessments and the useful preparation for potential events. This requires what Karl Weick[44] and others have labeled mindfulness – tools and culture that encourage the examination of fault lines, a focus on mistakes, a sense of the key operational variables in any given environment, and the capacity of information to flow freely throughout the system. This is a big challenge when one looks at the CI landscape in Canada.

Another emergent theme for CI protection, and one that has been learned in many fields engaged in emergency planning and response, is that no one tool fixes all problems. Because of the dynamic nature of threats to CI, settling on a single strategy of protection is an invitation to disaster. Once that strategy is detected and understood, it is easy to get around it. As the nature of threats change and come up with annoying surprises that do not fit the documented emergency plan, organizations have to adapt. Hence, there is core value to build internal challenge functions into CI assessments. Further, the value of sharing information through research, industry associations, and broader government challenges is much more than a "nice to have". It is a "have to have". Within the confines of real security issues, there needs to be a wider accessibility to information on CI protection, on the nature of threats as they emerge, and on innovative (or even good old reliable) responses. To that end, building on what has already been done, increased efforts need to be put into creating what Nobel Laureate Elinor Ostrom[45] of MIT calls the *knowledge commons* as a key resource in combating CI threats. Such a commons has to be inter-disciplinary and inter-jurisdictional. It is clear that various sectors experience CI threats differently, but there remain powerful common threads, especially around cyber threats and infrastructure degradation, which beg to be shared.

The level of awareness of CI threats and risks is certainly elevated. Both governments and the private sector are acting on them, if in different ways at times. What is important is that this be seen as a permanent state, not simply the result of some episodic activity by terrorists. The reason this is important is that much of the threat to CI does not lie simply in agent activity. The core to the vulnerability in virtually all sectors is the emerging complexity and interdependence within sectors and across them. To a degree this reflects the overlay of cyber-dependence within all systems. Added to this is the complexity of remote control systems that can themselves be seen as vulnerable to both attack and degradation. All CI systems have become more complex and more open to error, misfiring, or attack with consequences that are unintended and possibly even unknowable until they occur.

The current Canadian approach to CI recognizes that command and control approaches, based on regulation and oversight are not workable and are expensive.

The current Canadian approach to CI recognizes that a command and control approach, driven by government regulation and oversight, is not workable, let along affordable. Governments therefore, while operating key sub-systems, must rely increasingly on collaboration, partnerships, and the willing engagement of other sub-system owners. What government can bring to the table is the overlay of communications, information, and connectivity of these sub-systems. It must nurture the culture of mindfulness with improved intelligence sharing, challenging the status quo. It must also be prepared to look into new ways of doing things, search out leading practice in other jurisdictions and find ways to effectively disseminate those products in a useful way to both sub-system owners and to the reliable professionals working within them. This means investing in research and working with professional organizations associated with CI personnel.

Are we safe enough? We can only answer that question by continually asking it. There is no end state here. All actors in the system have to realize that.

CRITICAL INFRASTRUCTURE PROTECTION: AN ANNOTATED BIBLIOGRAPHY

This Bibliography was prepared by Research Assistant Scott McFatridge with modifications by the author.

North America

Baker, Steward, Natalia Filipiak, and Katrina Timlin. 2011. *In the Dark: Critical Industries Confront Cyberattacks.* Centre for Strategic and International Studies and McAfee, Inc. Available from: http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure- protection.pdf – Focuses on the risks of cyber-attacks faced by critical infrastructure in the oil, gas, power and water utilities. The report emphasizes that rather only minor improvements to security have been made, despite increasing threats and vulnerabilities facing these sectors.

Electric Energy T&D Magazine Editorial Staff. November/December 2008. *Securing Utility Assets: The Ways and Means of Critical Infrastructure Protection (Part 1)*. Electric Energy Online. Available from: http://www.electricenergyonline.com/page=show_article&mag=&article=401 – A round-table discussion on critical infrastructure protection by security experts in the electricity industry. This segment focuses on private sector best practices for cyber-infrastructure protection.

Electric Energy T&D Magazine Editorial Staff. January/February 2009. *Securing Utility Assets: The Ways and Means of Critical Infrastructure Protection (Part 2)*. Electric Energy Online. Electric Energy Online. Available from: http://www.electricenergyonline.com/? page=show_article&mag=&article=398 – A round-table discussion on critical infrastructure protection by security experts in the electricity industry. Part 2 focuses on private sector best practices for the protection of physical infrastructure.

Homeland Security and Public Safety Canada. 2010. *Canada-United States Action Plan for Critical Infrastructure.* Available from: http://www.dhs.gov/xlibrary/assets/ ip_canada_us_action_plan.pdf – A non-binding action plan for cooperation between the Canadian and US governments. Recommended actions include the creation of "a virtual Canada-U.S. Infrastructure Risk Analysis Cell", enhancing sector-specific cross border collaboration, further information sharing, and collaboration on risk assessment and identification of priority areas.

North American Electric Reliability Corp. 2010. *Action Plan to Mitigate Against High-Impact, Low-Frequency Event Risks.* Available from: http://nerc.com/files/HILF.pdf – Discusses four high-impact, low-frequency scenarios for critical infrastructure threats: coordinated physical, cyber or blended attack risk and pandemic risk, as well as geomagnetic disturbances, high altitude electromagnetic pulse events, and intentional electromagnetic interference threats and various options for mitigating these risks, and proposes an action plan (further elaborated in the sequel document; see below).

North American Electric Reliability Corp. 2010. *Critical Infrastructure Strategic Initiatives Coordinated Action Plan.* Available from: http://www.nerc.com/docs/ciscap/Critical_Infrastructure_Strategic_Initiatives_Coordinated_Action_Plan_102510.pdf – The Action Plan outlines four severe-impact scenarios for high-impact, low frequency events, strategic initiatives which draw on the scenarios for recommendations, and a detailed action plan for each initiative.

Weatherford, Mark. October 2010. *'Unknown unknowns' and the electric grid*. SC Magazine. Available from: http://www.scmagazineus.com/unknown-unknowns-and-the-electric-grid/article/181292/ – Article discussing the interconnectedness and vulnerabilities of the North American electricity grid, and recent steps taken by the North American Electric Reliability Corp. after the release of their *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System* report.

Canada Bradley, Francis. March/April 2003. *Critical Infrastructure Protection: A Priority for Industry.* Electric Energy Online. http://www.electricenergyonline.com/ page=show_article&mag=12&article=84 – Discusses post-September 11 measures taken by the CEA to protect critical electricity infrastructure, with an emphasis on cyber-attacks to infrastructure.

Centre for Infrastructure Protection and Homeland Security. 2002-2011. *The CIP Report.* Available from: http://cip.gmu.edu/publications/books. – Archives and the current issue of a monthly newsletter on critical infrastructure protection, which, over the course of 9 years, has covered nearly every critical infrastructure sector imaginable.

McCrank, Neil. October 2006. *Protecting Alberta's Critical Energy Infrastructure.* Vanguard Magazine. Available from: http://www.vanguardcanada.com/CriticalInfrastructureMcCrank – Discusses the steps taken to protect Alberta's Critical Energy Infrastructure in the wake of September 11, with an emphasis on the role of the EUB.

Public Safety Canada. 2008. *Towards a National Strategy and Action Plan for Critical Infrastructure.* Available through http://www.weao.org Publication outlining the national strategy and action plan for critical infrastructure protection in Canada. Notes, “an accurate assessment of the state of readiness [at the time of publication] of each sector is difficult” (Action Plan, p. 18). Actions taken include the establishment of a National Cross-Sector Forum, the creation of inter-jurisdictional and inter-sectoral information-sharing networks, and a framework for the continued review and revision of the Action Plan. Also notes that “each sector network will address cyber risks and dependencies” (Action Plan, p. 15).

Shull, Aron. January 21, 2011. *How Secure is Canada's Energy Infrastructure?* The Mark. Available from: http://www.themarknews.com/articles/3794-how-secure-is-canada-s-energy-infrastructure – A fairly critical editorial arguing that Canada should do more to protect its critical infrastructure, and that steps could have been taken much sooner.

Stebila, Douglas. March 2010. *The Rise of Denial of Service Attacks*. Vanguard Magazine. Available from: http://www.vanguardcanada.com/DenialOfServiceAttacksStebila – A discussion of the challenges inherent in preventing and preparing for Distributed Denial of Service Attacks, due to the dispersed nature of both the bots and the control infrastructure, and also in light of the fact that the former are often located in multiple jurisdictions.

Thatcher, Chris. September 2008. *Critical Protection: Collection of Suspicious Incidents Strengthens Partnerships.* Vanguard Magazine. Available from: http://www.vanguardcanada.com/CriticalProtectionCICIThatcher – Discusses the inception and future directions of the RCMP's electronic suspicious incident reporting system.

Thatcher, Chris. February 2011. *Critical Strategy: Infrastructure Protection in the Cyber Domain.* Vanguard Magazine. Available from: http://www.vanguardcanada.com/Critical ThreatRCMPThatcher – Outlines recent steps taken by the RCMP towards information-sharing between the public and private sectors in Canada, as well as between Canada and the United States, for purposes of protecting Canada's cyber-infrastructure.

Vanguard Editorial Staff. September 2009. *Cross-border collaboration: a call to close cyber, critical infrastructure gaps.* Vanguard Magazine. Available from: http://www.vanguardcanada.com/CrossBorderCollaborationRidge – Interview with then-First Secretary of Homeland Security in which he discusses how critical infrastructure protection has receded on the political agenda, and the need to develop a broadband safety network for public security, among other topics.

The United States

Eisenhauer, Jack, Paget Donnelly, Mark Ellis, and Michael O'Brien. 2006. *Roadmap to secure control systems in the Energy Sector.* U.S. Department of Homeland Security. Available through http://www.oe.energy.gov – Outlines a strategic framework for 2015 for securing control systems in the energy sector, including automated monitoring of their control system networks with real-time response capacities, the implementation of next-generation control systems with automated contingency and threat response functions, and continued collaboration between the federal government and private owners of infrastructure assets.

U.S. Department of Homeland Security. May 2007. *Energy: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan (Redacted)*. Available from http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-redacted.pdf- Provides a comprehensive assessment of risks facing critical infrastructure in the energy sector, as well as the protective actions and performance measurements that have been put into place.

National Infrastructure Advisory Council. September 2009. *Critical Infrastructure Resilience: Final Report and Recommendations.* Available from: http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf – The report concludes that the overall policy framework for critical infrastructure protection in the Unites States is sound, but that greater emphasis ought to be placed on the concept of resilience. It argues that the federal government should play a co-operative role with the private sector by creating incentives for greater resilience for owners of private critical infrastructure, but acknowledges that more direct government involvement will be needed to hedge against the effects of high-impact, low-frequency events.

Oltsik, Jon, John McKnight and Jennifer Gahm. November 2010. *A report on Assessing Cyber Supply Chain Security Vulnerabilities Within the U.S. Critical Infrastructure.* Enterprise Strategy Group and the U.S. Department of Homeland Security. Available from: http://www.enterprisestrategygroup.com/media/wordpress/2010/11/ESG-Research-Report-Cyber-Supply-Chain-Security-Nov-10.pdf – Based on a comprehensive survey of cyber security practices in a number of critical infrastructure areas, the report concludes that critical infrastructure is facing repeated and ongoing cyber attack, and that threats of these attacks are mounting. On the other hand, they found a close connection between cyber security and regulatory compliance, and they also found evidence that critical infrastructure sectors would like more government assistance in fostering cyber security.

Sweden

Swedish Defence Research Agency. 2005. *Critical Information Infrastructure Protection: A Swedish Perspective.* Available from: http://www2.foi.se/rapp/foir1549.pdf – Discusses the vulnerabilities facing Sweden's critical information infrastructure, the organizational architecture and mechanisms in place to protect it, and the methods used to trace network-mediated attacks from inside and outside the country.

European Union

Crisis and Risk Network and the Centre for Security Studies. 2008. *CRN Focal Report 1: Critical Infrastructure Protection.* Swiss Federal Office of Civil Protection. The first half of the report provides an overview in recent CIP trends from the European Union (including Sweden), the United States, and Canada, and the second half places specific emphasis on the physical protection of critical energy infrastructure. Available through http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home.html.

ENDNOTES

[1] Available at http://www.publicsafety.gc.ca/prg/em/ci/ntnl-eng.aspx, accessed August 2011.

[2] Canada: About Critical Infrastructure, Public Safety Canada, accessed June 2011, www.ps-sp.gc.ca.

[3] Available at http://www.publicsafety.gc.ca/prg/em/ci/ntnl-eng.aspx, accessed August 2011.

[4] Canada: About Critical Infrastructure, Public Safety Canada, accessed June 2011, www.ps-sp.gc.ca.

[5] Author interview.

[6] Auditor General of Canada, *2009 Annual Report, Chapter 7: Emergency Management*, p. 21.

[7] See http://www.cepa.com/map/.

[8] *Op. cit.*

[9] The rich literature in this area is summarized in Camillus, J.C. 2008. "Strategy as a Wicked Problem," *Harvard Business Review*, Vol. 86, 98-101.

[10] |See Horn, Robert E. and Robert P. Weber. 2007. *New Tools For Resolving Wicked Problems: Mess Mapping and Resolution Mapping Processes.* Strategy Kinetics L.L.C.

[11] Information provided by Public Safety officials, August 2011.

[12] "Costly Hydro Towers Sit Idle," *Toronto Sun*, Feb. 28, 2011. Available at http://www.torontosun.com/news/canada/2011/02/28/17442741.html, accessed July 2011.

[13] "RCMP urge patience in B.C. pipeline bomb probe," *Canada Press*, July 5, 2009. Available at http://www.cbc.ca/news/canada/british-columbia/story/2009/07/05/bc-dawson-creek-sixth-pipeline-bombing.html, accessed September 2011.

[14] "Ludwig's arrest may have had more to do with Olympics than evidence," *The Edmonton Journal,* January 2010. Available at http://www2.canada.com/edmontonjournal/news/opinion/story.html?id=6fd554b9-cdf8-41a3-9f4b-a99e5bd1b507&p=2, accessed September 2011.

[15] Conference Board of Canada. 2006. *Facing Risks: Global Security Trends and Canada*. Ottawa: Conference Board of Canada.

[16] Jacques J. M. Shore. 2008. "The Legal Imperative to Protect Critical Energy Infrastructure," *Critical Energy Infrastructure Protection Policy Research Series, No. 2*. Carleton Centre of Intelligence and Security Studies.

[17] *National Strategy, op.cit.* p. 8.

18 Dan Gardner. 2008. Risk: *The Science and Politics of Fear*. McClelland.

19 Center for Nonproliferation Studies, Monterey Institute of International Studies. 2007. *Assessing Terrorist Motivations for Attacking Critical Infrastructure*. Available at www.llnl.gov/tid/lof/documents/pdf/341566.pdf, accessed July 2011.

20 "Natives in Canada Barricade Railway in Fight for Land," *The Militant*, Vol. 71. No 19, May, 2007.

21 Public Safety Canada.2004. *Threats to Canada's Critical Infrastructure.* Available at www.publicsafety.gc.ca/prg/em/ccirc/_fl/ta03-001-eng.pdf, accessed July 2011.

22 Interview with senior Hydro One officials.

23 Daily Commercial news and construction record. May 1, 2008. "As copper prices rise, theft problem grows, police say." Available at http://dcnonl.com/article/id27470, accessed July 2011.

24 http://globalguerrillas.typepad.com/globalguerrillas/2004/05/design_flaws_wh.html accessed August 2011.

25 Department of Homeland Security. 2008. *The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures.* Available at www.dhs.gov/.../niac_insider_threat_to_critical_infrastructures_study.pdf, accessed July 2011.

26 *Ibid*. p. 5.

27 Nancy J. Wong. 2002. "National Critical Infrastructure Protection: A Context and Framework for the Electric Industry." Critical Infrastructure Assurance Office presentation.

28 Canada, Public Safety and Emergency Preparedness Canada (PSEPC). 2002. *National Critical Infrastructure Assurance Program,* Ottawa: PSEPC. ww.publicsafety.gc.ca/prg/em/nciap/index-eng.aspx. This materal is archived but described in a 2008 report by the Department of Finance, to be found at http://www.fin.gc.ca/treas/evaluations/epcip-piepc-eng.asp. See Section 2.1.1.

29 Many of these documents from the early 2000s are difficult to find on the Public Safety Canada website. This 2004 policy statement was sourced through a web search at www.acpa-ports.net/advocacy/pdfs/nscip_e.pdf.

30 Auditor General of Canada. 2005. *2005 Annual Report:. National Security in Canada*. Chapter 2.

31 Andrew Graham, presentation, available at http://post.queensu.ca/~grahama/presentations/EMERGPREP.pdf.

32 Available at http://www.publicsafety.gc.ca/prg/em/ci/cnus-ct-pln-eng.aspx, accessed July 2011.

33 Available at www.conferenceboard.ca.

34 Martin Rudner. 2006. "Protecting North America's Energy Infrastructure Against Terrorism." *International Journal Of Intelligence and Counter Intelligence*.

35 Shore, *op. cit*., p. 11.

36 Personal interview.

37 Mr. Reicher's presentation can be found at http://www.slideshare.net/aboutpipelines/cepa-state-of-the-pipeline-industry , accessed August, 2011.

38 For more information, see http://www.css.drdc-rddc.gc.ca/about-sujet/index-eng.asp.

39 Nassim Nicholas Taleb. 2007. *The Black Swan.* Random House.

40 http://www.vanguardcanada.com/CyberStrategyRobertDick.

41 Interviews with federal officials.

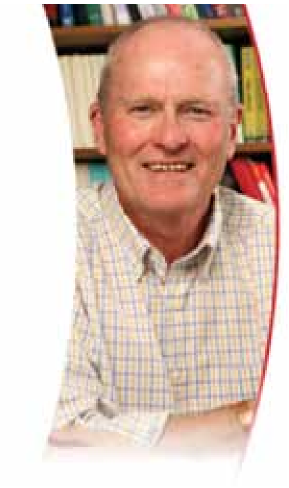
42 Andrew Archibald and Gilles Rheaume. April 2009. *Building Resilience: Cooperation and Coordination of an Effective Response.* Conference Board of Canada.

43 Homeland Security Advisory Council. 2006. *Report of the Critical Infrastructure Task Force*. Washington, D.C.: U.S. Department of Homeland Security. p. iii. Available at www.dhs.gov/xlibrary/assets/HSAC_CITF_Report_v2.pdf, accessed August 2011.

44 Karl Weick and Kathleen Sutcliffe. 2001. *Managing the Unexpected*. Jossey-Bass.

45 Charlotte Hess and Elinor Ostrom (eds.). 2006. *Understanding Knowledge as a Commons*. MIT Press.

ABOUT THE AUTHOR



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 Masters 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 for 14 years in the federal government.

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.

THE HILL TIMES

The Economist

and in other major Canadian and international media

www.macdonaldlaurier.ca