THE CIP EXCHANGE

A forum for sharing views and information about critical infrastructure protection SPRING 2008

The Worst of Times

Cass Sunstein discusses worst-case scenarios and the precautionary principle

DALHOUSIE UNIVERSITY Inspiring Minds | Faculty of Management | School of Public Administration

CONTENTS

EDITORIAL

Editor: Kevin Quigley

Assistant Editor: Julie Davies

Copy Editing (French Language): Marie Tounissoux

Design: Dalhousie Design Services, Roxanna Boers, Designer

Additional Thanks: Ron Pelot, Director, Centre for Risk Management at Dalhousie

A leading public intellectual, Cass R. Sunstein is the author or co-author of more than 15 books and hundreds of scholarly articles. He has written extensively on many aspects of public law, including the regulation of risk, and is the most cited law professor on any law faculty in the United States. Sunstein is currently the Karl N. Llewellyn Distinguished Service Professor of Jurisprudence, a joint appointment of the law school and Political Science Department at the University of Chicago. In fall 2008, Sunstein will join the Harvard Law School faculty where he will also become director of the new Program on Risk Regulation. In 2007, he published *Worst-Case Scenarios* with Harvard University Press. Kevin Quigley interviewed Cass Sunstein last December.

KQ: Is it useful for policy-makers who are responsible for the protection of critical infrastructure to think in terms of worst-case scenarios?

CS: Certainly – but don't get carried away! If the worst-case scenario is highly unlikely to occur, it might not be worth a ton of attention. We need to think both about outcomes *and* about their probabilities. If the worst-case scenario would occur only if there's a miracle – like Martians landing – we shouldn't worry about it. But if the risk is real – like a terrorist attack or a hurricane – by all means we need to plan for it.

Cass Sunstein

KQ: When we plan to protect our critical infrastructure, does it matter if we anticipate terrorist attacks as opposed to natural disasters?

CS: Well, our plans will differ, depending on what the source of the risk is, but the analysis is very close. We certainly should take prudent precautions against all sorts of risks. Cost-benefit analysis can be very helpful here. It doesn't make sense to close down the airline industry to reduce the risk of terrorism. The cost of doing that is simply too high.

KQ: Given our dependence on complex technologies and intricate global

For information on the June 3rd CIP Workshop at Dalhousie, see pages 15-17

supply chains, is it possible to assign accurate probabilities to low-probability, high-consequence failures in critical infrastructure?

CS: Often it is not. But we should try to do the best we can. When we can't make a point estimate (e.g., a 1% likelihood), we can often specify a range (e.g., higher than 1%, but lower than 20%). One of the highest priorities in the modern era is to try to be as precise as possible about the magnitude of risks, and we're learning more all the time.

KQ: Are cost-benefit analyses effective mechanisms for determining where to focus our efforts in matters of critical infrastructure protection?

> A great failure of governance, before 9/11, was a failure to take precautions that most experts favoured.

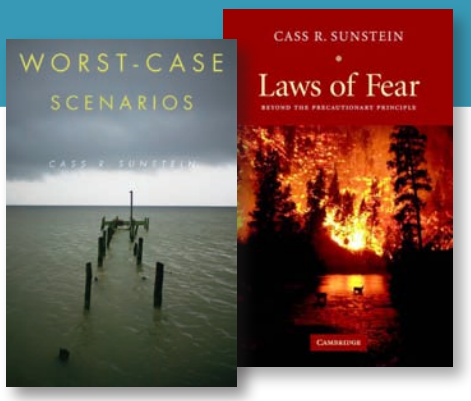
CS: Yes, if they're done properly. We need to know the size of the risks *and* the burdens imposed by reducing them. Cost-benefit analysis is the best way to accumulate the necessary information and to help us to decide what to do. If attention is paid to getting the analysis right, we'll have a much better sense of what we ought to be doing.

KQ: In *Worst-Case Scenarios* and in a recent interview with Russ Roberts (econtalk.org), you noted that on September 10th, 2001, Americans would not have supported the security measures they now face when they try to board an airplane. You attribute their pre-September 11th behaviour to the absence of an availability heuristic.[1] Is there a way to prompt populations to react before such a focusing event, or is a focusing event required?

CS: For populations, a focusing event will be required if people begin with initial skepticism about the existence or magnitude of the risk and if reducing the risk imposes significant burdens. But ours is a republic, not a direct democracy, and sometimes experts can encourage the government to take precautions even if the public is not alarmed. Private and public institutions can and do act even without a focusing event. A great failure of governance, before 9/11, was a failure to take precautions that most experts favoured.

KQ: In *Worst-Case Scenarios* and *Laws of Fear: Beyond the Precautionary Principle*, you argue that there is an internal contradiction within the precautionary principle which, by its very nature, prevents the actions it requires. Can you envision a context in which the principle or an application of the principle might be useful?

CS: The problem is that the precautionary principle forbids the very steps that it requires, because precautions themselves create risks. If the precautionary principle says that we should build a margin of safety into all decisions, there's a problem: risks are on all sides, and so it's hard to have a margin of safety against all risks! If you stay home, you create risks; so too, if you go to work; so too, if you exercise; so too, if you don't exercise. The Iraq War was plausibly defended partly on precautionary grounds; it was plausibly criticized on those same grounds. Aggressive steps to prevent climate change are plausibly defended on precautionary grounds, but such steps might well violate the precautionary principle because they too create risks. We can imagine steps involving critical infrastructure that are required by the principle – but that also offend it, because they impose costs and create risks of their own.



Selected publications by Cass Sunstein

On the other hand, *Worst-Case Scenarios* does explore certain, more refined versions of the precautionary principle, including the Irreversible Harm Precautionary Principle and the Catastrophic Harm Precautionary Principle. Both of these have uses in particular contexts. An elaboration would take a lot of space, but the basic idea is that it does make sense to take special precautions against irreversible harms and against genuine catastrophes. What precautions are special? Alas, you'll have to read the book to find out!

The Program on Risk Regulation at Harvard will focus on how law and policy deal with the central hazards of the 21st century. Anticipated areas of study include terrorism, climate change, occupational safety, infectious diseases, natural disasters, and other low-probability, high-consequence events. Kevin Quigley conducted this interview via email on December 18th, 2007. Notes from the introduction were taken from the Harvard Law School website. For a current profile of Cass Sunstein, please refer to his faculty webpage: http://www.law.uchicago.edu/faculty/sunstein/

[1] "It is well established that in thinking about risks, people rely on certain heuristics, or rules of thumb, which serve to simplify their inquiry… When people use the availability heuristic, they assess the magnitude of risks by asking whether examples can readily come to mind." Quoted from *Laws of Fear: Beyond the Precautionary Principle (The Seeley Lectures)* by Cass R. Sunstein, page 36 in the 2005 hardcover edition from Cambridge University Press.

Interview with
Gloria Kuffner

CIO at the Canada Revenue Agency

Taxing Times

Gloria Kuffner shares her experience from 2007 when a software defect forced the CRA to take its systems offline at one of the busiest times of the year

On March 6th, 2007, the Canada Revenue Agency (CRA) was forced to take its systems offline for nine days due to a defect in a vendor's software package. The CRA typically processes 3.21 million transactions hourly and $1.3 billion each business day; the resulting disruption received national and international media coverage. Gloria Kuffner first joined the CRA in 1980 and became CIO in 2006. Kevin Quigley interviewed Gloria Kuffner in March, one year after the outage.

KQ: In many respects, the CRA has had an ambitious IT strategy for a number of years. Much of the organization's key functions now depend extensively on IT infrastructure. The network of actors involved in managing this infrastructure is vast, and many of the players reside organizationally or physically outside of the CRA. Given this context how do you ensure the external expertise on which you rely is dependable?

GK: We work really hard to maintain strong working relationships with other government agencies and the many vendors that provide us with products and services. We develop these relationships over many years. Our long-term partners are typically recognized industry leaders with proven track records. In addition, in selecting any particular product, the CRA goes through a comprehensive evaluation, not only of the IT component or product or service being supplied, but also of the IT organization that will be delivering that portion of our IT infrastructure. Finally, when we enter into a contract with a private industry partner, we are very specific about the performance requirements that we expect. We also have contingency plans in place should that level of service not be provided.

KQ: What did you learn about risk management during the 2007 outage? If confronted with a similar issue, what would you do differently?

GK: Obviously, we hope never to be in that same situation again. An independent, third-party review concluded that multiple factors contributed to this failure, and that it would have been nearly impossible to anticipate. We had undergone a very rigorous assessment before we carried out the change that caused the problem. In fact, we put this particular software through six different test environments and were unable to detect the defect. After the incident was over, we talked to the vendor about what processes they would put in place to increase the quality of the products they send to us.

> The response must consider and manage a number of factors, from political and legal implications to communications and security.

Gloria Kuffner

Our review confirmed what we already knew—business continuity, business resumption and disaster recovery programs are invaluable. It was also important to have a robust monitoring and incident management process. That worked very well for us—the software anomaly was detected and reported up through our management team very rapidly. We also confirmed that you need to have strong leadership in place during a

Canada Revenue Agency by the Numbers:

- 3.21 million transactions processed hourly
- $330 billion collected annually
- 25 million individual tax returns processed annually
- $14.7 billion distributed in individual benefit and credit payments

time of crisis. Communication at all levels was absolutely critical—within the IT organization, the Agency, and to all stakeholders.

KQ: Operational crises or emergencies, if we could describe the outage in those terms, involve numerous departments and agencies across government. What lesson did you draw from the outage about the governance of an operational crisis or emergency?

GK: The response must consider and manage a number of factors, from political and legal implications to communications and security. The more you can do to prepare for how communications should work during a time of crisis, the better. It is really important that we have clear government-wide incident management processes, protocols and mechanisms in place.

We also need to ensure that, when appropriate, decisions must be taken from a government-wide perspective and not just a departmental perspective. We may have to look at prioritizing the services provided by the Government of Canada. In times of crisis, we may find that more than one government entity is impacted and therefore the recovery plan will have to consider which services need to be recovered first.

KQ: What do you see as the biggest risk for the Government of Canada going forward in a networked environment that is increasingly dependent on IT?

GK: As the Government of Canada becomes more interdependent, we will have more stakeholders; this requires more collaboration and consultation. In times of crisis, however, we need to make decisions *quickly*. The more that we can do in advance to prepare for certain scenarios, the better equipped we will be to respond in a timely and effective manner.

KQ: Is it feasible to think we can put effective emergency management practices in place in advance? There is always an element of surprise in these situations.

GK: We have to develop the decision-making capability within our own workforce. When 'non-crisis' operational failures arise, we (at the CRA) ask individuals with expertise in that particular area for their analysis of the situation and a recommended course of action. In a sense, we train people by having these types of discussions. Can we have a similar approach across government? Absolutely. I wouldn't necessarily say we've spent as much time having those discussions as we need to, but I believe it's possible to put in place a decision-making framework.

KQ: When I was doing my research for this interview, I was surprised by the relatively small amount of media coverage for what could be considered such a serious issue.

GK: Our commissioner immediately went to the media to explain exactly what we knew and that we didn't have all the answers yet. I think people respect that level of honesty and the fact that we came forward immediately. I also think that we have built up a significant level of trust with Canadians and I believe that foundation of trust can carry you through difficult times.

KQ: So what do you think the lasting impact of this event will be?

GK: Last year we had more people file online than we've ever had in past years. It didn't have any immediate impact in that respect. There was considerable interest in learning from this event, however. I had a number of people calling me—governments from around the world, in fact, contacted us eager to learn from our experience. I also met with a number of CIOs at our North America Day where we convene with governments from the United States and Mexico. Within the Government of Canada, we've had discussions about learning from this particular experience with Public Safety Canada and the Treasury Board Secretariat. So it does have a lasting effect, I would say.

We have to develop the **decision-making capability** within our own workforce.

Kevin Quigley interviewed Gloria Kuffner on March 7th, 2008 in her Ottawa office. This text has been edited for publication.

The Domino Effect

The *Centre risque & performance* at the *École Polytechnique de Montréal* focuses on avoiding potential domino effects generated by single critical infrastructure failure

by Benoît Robert & Luciano Morabito

Founded in 1998 at the *École Polytechnique de Montréal*, the *Centre risque & performance* (CRP) focuses on interdependencies among critical infrastructure systems. Over the years, this issue has become a major challenge for industrial societies since the failure of any one system can trigger multiple failures across several systems with serious consequences for the economy, the environment and society.

For the past decade, the CRP has been working in partnership with key stakeholders in Quebec, including private industry as well as municipal, provincial and federal governments,

> "Domino effects curves are the most notable result emerging from the CRP's research."

on a new methodology for assessing and managing interdependencies among critical infrastructure systems. Currently, the CRP is studying Montréal and Québec City where it has established a cooperative space in which managers of critical infrastructure can exchange confidential information in order to create an effective method to identify and characterize these functional interdependencies.[1] This collaboration will allow the CRP and all stakeholders to anticipate better any domino effects between critical infrastructure systems and to develop measures of prevention and protection while facilitating communication and early intervention in emergency situations.

The methodology developed by the CRP is based on the exchange of resources between critical infrastructure systems in provider/supplier relationships that consequently generate functional interdependencies. When a resource is no longer usable (due to deterioration or inaccessibility), it affects any critical infrastructure system using it. The level to which a system is affected depends on its reliance on that first resource and the availability of alternative resources. The failure of this second compromised infrastructure then leads to the deterioration or inaccessibility of the resource or service that system itself provides. This creates a domino effect or chain reaction where the failure of one system results in the failure of another system, and so on…

Benoît Robert

To illustrate the reliance of critical infrastructure systems on the resources they use, the CRP has created dependency curves (Figure 1). These curves express the level to which the resource—when unavailable—affects the various systems that are using it as a function of time and space. The state of each system is represented by indicators ranging from green (where the system functions normally) to red (where the system no longer supplies its own resource to one or more areas of the study zone). Developed for each resource affecting critical infrastructure systems, these curves demonstrate the system's level of

[1] See Robert, B., Morabito, L. and Quenneville, O. (2007). "The preventive approach to risks related to interdependent infrastructures," *International Journal of Emergency Management*, Vol. 4, No. 2, pp.166–182.

Figure 1:
Example of Dependency Curves

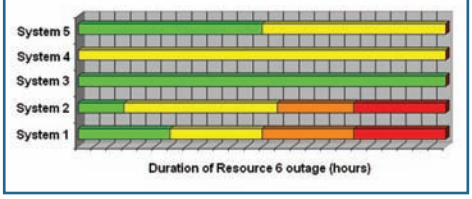
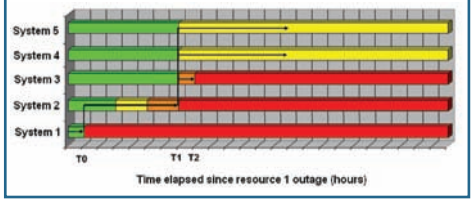


Figure 2:
Example of Domino Effects Curves



tolerance when it is faced with the unavailability of a particular resource.

To design these curves, each critical infrastructure system must identify the resources they use at various stages and the consequences (as a function of time) of the unavailability of each resource on its system. These consequences are expressed in terms of the system's capacity to fulfill its mission. It is then possible to create dependencies curves for each critical infrastructure and for each resource. Whenever a resource is no longer available, it is then possible to identify which systems will be affected and the potential consequences on the critical infrastructure as a whole. Since a resource problem rarely affects an entire city or municipality, the CRP concentrates on areas of one square kilometre.

Domino effects curves are the most notable result emerging from the CRP's research. These curves are obtained by combining dependency curves. For example, in Figure 2, when System 1 fails at T0, it generates a domino effect on System 2. After a certain period of time (T1 – T0), System 2 will fail and generate a domino effect on Systems 3, 4 and 5. The effect on Systems 4 and 5 in this situation will be minimal, but System 3 will fail shortly thereafter at T2.

Clearly, these curves can identify potential domino effects resulting from the degradation or unavailability of a resource in a particular area. This allows the managers of critical infrastructure systems to anticipate potential domino effects, prioritize interdependencies according to specific criteria and evaluate any system's tolerance relative to its resources.

After 10 years of research, the methodology and resulting data distinguishes the CRP from other research teams, both in Canada and internationally. These results lay the groundwork for the creation of an early warning system for real-time management of interdependencies among critical infrastructure systems. The goal is to model interdependencies between these organizations and to develop real-time systems capable of anticipating domino effects. Future CRP projects will deal specifically with this problem of modeling interdependencies among critical infrastructure systems as well as address the issue of geographical interdependencies among these systems.

Dr. Benoît Robert is the founder of the *Centre risque & performance* and Associate Professor with the Department of Mathematical and Industrial Engineering at the *École Polytechnique de Montréal*. Luciano Morabito is a research associate with the *Centre risque & performance*. For more information, please visit www.polymtl.ca/crp or contact Luciano Morabito – (514) 340-4711 (#2271), luciano.morabito@polymtl.ca or Benoît Robert – (514) 340-4711 (#4226), benoit.robert@polymtl.ca.

"These curves allow... managers of critical infrastructure systems to anticipate potential domino effects, prioritize interdependencies according to specific criteria and evaluate any system's tolerance relative to its resources."

École Polytechnique de Montréal

Les effets domino

Le Centre risque & performance de l'École Polytechnique de Montréal a pour mission d'éviter les effets dominos pouvant potentiellement être générés par la défaillance d'une seule infrastructure essentielle.

par Benoît Robert et Luciano Morabito

Benoît Robert

Fondé en 1998 à l'École Polytechnique de Montréal, le Centre risque & performance (CRP) concentre ses travaux de recherche sur les interdépendances entre les infrastructures essentielles (IE). Cette problématique est devenue, au fil des ans, un enjeu majeur pour nos sociétés industrielles. Ceci parce que la défaillance d'une seule de ces IE peut générer un effet domino sur les autres IE et avoir de sérieuses conséquences pour l'économie, l'environnement et la société.

Depuis maintenant une dizaine d'années, le CRP travaille à développer une méthodologie d'évaluation et de gestion des interdépendances entre les IE. Le CRP travaille en partenariat avec les principales IE du Québec et les gouvernements provincial et fédéral. Les deux villes actuellement étudiées sont Montréal et Québec. Dans ces villes, un espace de coopération où les gestionnaires des IE s'échangent, dans un cadre de confidentialité, des informations pertinentes à la gestion de leurs interdépendances, a été mis sur pied. Du travail de ce groupe d'experts est née une méthodologie efficace et opérationnelle permettant d'identifier et de caractériser les interdépendances fonctionnelles entre les IE[1], d'anticiper les effets domino entre les IE, de mettre en place des mesures de prévention et de protection face à ces effets domino et de faciliter les communications et les interventions en situation d'urgence. Ces résultats permettent aux gestionnaires des IE de mieux se préparer face aux risques inhérents aux interdépendances et leurs effets domino potentiels.

> « Les courbes d'effets domino constituent le résultat le plus significatif des travaux du CRP. »

La méthodologie développée par le CRP est basée sur l'échange de ressources entre les IE. Cet échange est à la base même des interdépendances fonctionnelles (relations clients/fournisseurs) entre les IE. Ainsi, lorsqu'une ressource n'est plus utilisable (parce que dégradée ou non disponible), cela affecte les IE qui utilisent cette ressource à un degré plus ou moins élevé, selon l'utilisation qui est faite de la ressource et selon la disponibilité de ressources alternatives. Un effet domino est alors initié lorsqu'une IE tombe en défaillance suite à la dégradation ou la non disponibilité d'une ressource qu'elle utilise. La défaillance de cette IE entraîne alors la dégradation ou la non disponibilité de la ressource ou du service qu'elle-même fourni. S'ensuit alors un mécanisme en chaîne, ou effet domino, où la défaillance d'une organisation entraîne la défaillance d'une autre organisation, et ainsi de suite…

Pour illustrer la dépendance des IE face aux ressources qu'elles utilisent, le CRP a créé les courbes de dépendance (Figure 1). Ces courbes permettent de connaître, en fonction du temps et de l'espace, l'état de la fourniture de la ressource d'une IE lorsqu'une

[1] Voir Robert, B., Morabito, L. et Quenneville, O. (2007). « The preventive approach to risks related to interdependent infrastructures », *International Journal of Emergency Management*, Vol. 4, No. 2, pp.166–182.

Figure 1:
Exemple de courbes de dépendance

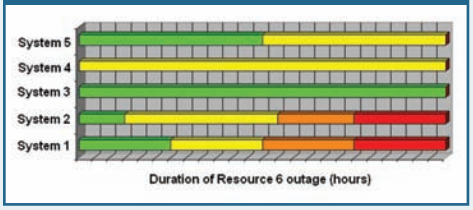
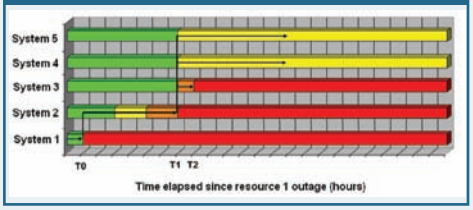


Figure 2:
Exemple de courbes d'effets domino



des ressources qu'elle utilise n'est plus disponible dans un secteur de la zone d'étude. Cet état est défini par des indicateurs variant du vert (la ressource est fournie normalement) au rouge (la ressource n'est plus fournie à un ou plusieurs des secteurs de la zone d'étude). Développées pour chacune des ressources fournies par les IE, ces courbes mettent en évidence le niveau de tolérance d'une IE face à la non disponibilité d'une ressource utilisée.

Pour construire ces courbes, chacune des IE doit identifier les ressources qu'elles utilisent pour leur fonctionnement ainsi que les conséquences, en fonction du temps, de la non disponibilité de chacune des ressources sur son propre réseau. Ces conséquences sont exprimées en fonction de la capacité du réseau à remplir sa mission. Il est alors possible de construire des courbes de dépendance pour chacune des ressources et pour chacune des infrastructures. Ainsi, lorsqu'une ressource n'est plus disponible, il est possible de connaître les réseaux qui en seront affectés, ainsi que les conséquences potentielles sur l'ensemble des IE. Puisque la dégradation ou la non disponibilité d'une ressource affecte rarement toute l'étendue d'une ville ou d'une municipalité, on fonctionne par secteurs. Dans le cadre des travaux du CRP, ces secteurs sont des quadrilatères d'un kilomètre carré.

Les courbes d'effets domino constituent le résultat le plus significatif des travaux du CRP. Elles sont obtenues en combinant l'ensemble des courbes de dépendances. Dans l'exemple de la figure 2, lorsque le système 1 entre en défaillance à l'instant T0, il engendre un premier effet domino sur le système 2. Après un certain temps (T1 – T0), le système 2 entrera en défaillance et générera ainsi un nouvel effet domino sur les systèmes 3, 4 et 5. Cette situation n'affectera pas de manière significative le fonctionnement des systèmes 4 et 5. Par contre, le système 3 entrera en défaillance peu de temps après (T2 – T1).

Comme on peut le constater, les courbes d'effets domino permettent l'identification systématique des effets domino potentiels qui résultent de la dégradation ou de la non disponibilité d'une ressource fournie dans un secteur particulier de la zone d'étude. Elles permettent de :

- anticiper les effets domino potentiels ;
- hiérarchiser les interdépendances en fonction de critères précis ;
- évaluer la tolérance des réseaux face à la défaillance d'une ressource utilisée.

Après 10 années de recherches, la méthodologie développée et les résultats obtenus permettent au CRP de se démarquer des autres équipes de recherche dans le domaine, tant au Canada que sur la scène internationale.

« Ces courbes permettent... aux gestionnaires des infrastructures essentielles d'anticiper les effets domino potentiels, de hiérarchiser les interdépendances en fonction de critères précis et d'évaluer la tolérance des réseaux face à la défaillance d'une ressource utilisée. »

École Polytechnique de Montréal

« Ces résultats ouvrent la voie à la création d'un système d'alerte rapide permettant la gestion en temps réel des interdépendances entre les infrastructures essentielles. »

Les résultats obtenus ouvrent la voie à la création de systèmes d'alerte précoce permettant la gestion en temps réel des interdépendances entre les IE. L'objectif est de modéliser les interdépendances entre les IE et de développer de réels tableaux de bords intelligents qui anticiperaient les phénomènes liés aux effets domino. Les prochains travaux du CRP porteront spécifiquement sur cette problématique de la modélisation des interdépendances entre les IE, en plus d'aborder la question des interdépendances géographiques.

Le Dr Benoît Robert est fondateur du Centre risque & performance et professeur associé au Département de mathématiques et génie industriel de l'École Polytechnique de Montréal. Luciano Morabito est associé de recherche au Centre risque & performance. Pour de plus amples informations, consultez www.polymtl.ca/crp ou communiquez avec Benoît Robert au (514) 340-4711 (poste 4226) ou à benoit.robert@polymtl.ca ou avec Luciano Morabito, au (514) 340-4711 (poste 2271) ou à luciano.morabito@polymtl.ca.

CRP Partners / Partenaires-clés du CRP

Bell Canada
Tecsult
GazMétro
Hydro-Québec
Ministère des Transports du Québec
Ministère de la Sécurité publique du Québec
Sécurité publique Canada
Ville de Montréal
Ville de Québec

Strengthening the Network

Public Security Technical Program at DRDC's Centre for Security Science seeks to identify & support *Communities of Practice* in key research areas, integrating expertise from academia, industry and government

by Andrew Vallerand

New, complex and emerging threats constantly require forward-looking solutions. Investments in science and technology (S&T) can improve and advance Canada's security capabilities to prevent and prepare, respond or recover from high-consequence safety and security threats, whether caused by terrorist or criminal activity, accidents, or natural disasters. Established in March 2006, the Public Security Technical Program (PSTP) is a joint initiative of Public Safety Canada and National Defence to develop a coordinated program to enhance collaboration, interoperability and capabilities across government using S&T as a lead investment. An upcoming open and transparent competition for best ideas including a Call for Proposal engaging government, industry and academia to deliver valued outcomes for public security partners and to address related capability gaps will further facilitate such investments.

Managed by the Centre for Security Science (CSS), PSTP complements the Chemical, Biological, Radiological-Nuclear, and Explosives (CBRNE) Research and Technology Initiative (CRTI Program), which is also managed by the CSS, by focusing on three addi-

tional areas or themes: Critical Infrastructure Protection (CIP), Surveillance, Intelligence and Interdiction (SI^2), and Emergency Management and Systems Integration (EMSI). Through PSTP, the Centre leverages existing S&T strengths in CBRNE domains with new resources to attempt to enhance capability gaps in these areas that may have been neglected in the past.

The purpose of the CIP component is to strengthen capabilities and to support the robustness, reliability, resilience, and protection of physical and information technology (IT) facilities, networks, services, and assets. Any disruption would have a serious impact on the health, safety, security, economic well-being, or effective functioning of the nation. The ten sectors that make up Canada's critical infrastructure are highly connected and interdependent. A failure of one sector could affect several others, resulting in a critical breakdown of essential services across Canada and potentially the U.S.

Therefore, to protect Canada's critical infrastructure, it is necessary to:

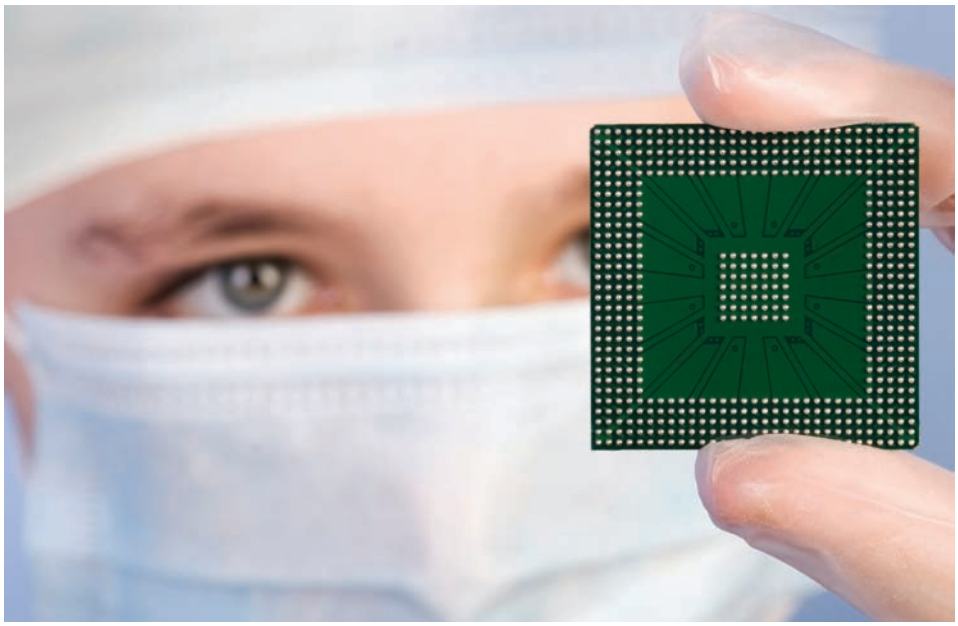
- Identify each new critical infrastructure system nationally, and develop and test new emergency management and business continuity plans;
- Using a scenario-based approach, assess hazards, threats, vulnerabilities and then risks to critical infrastructure;
- In conjunction with business continuity plans, assess and measure the "as is" capability and, in the presence of gaps that must be remediated, determine the road map to reach a "to be" capability;
- Identify the dependencies and interdependencies between infrastructures for given scenarios, and use analytical methods that model, simulate, anticipate and address the impact of such interconnectedness on key local nodes. If the removal of a key node influences assets related to energy, telecoms, water and transportation, to name a few, a "lifeline" may well be jeopardized. It is important to note here that resiliency or the ability to perform in a degraded state can be measured, and thus addressed. This is but one example of the value of S&T.

With partners across 21 federal departments and agencies, PSTP is also building *Communities of Practice* or 'clusters' around all three of its CIP, SI^2 and EMSI themes. This will create networks and partnerships that will integrate mandates, knowledge and expertise with representatives, as appropriate, from policy, requirements, S&T, and end-users/responders. Normally, this process spans government and, as appropriate, in an open and fair manner, academia and industry. Further discussions are taking place with these communities to define and recommend initial priorities for S&T activities around capability gaps for the forthcoming competitive Call for Proposals planned for fall 2008. Key areas of focus in critical infrastructure protection include:

- Infrastructure Vulnerability Assessment and Monitoring; and Infrastructure Resiliency;
- Natural Disaster Alert and Mitigation; and
- E-Security.

Recognizing the importance of strengthening collaboration between departments and agencies through joint projects that include academic and industry innovators in the field of science and technology, PSTP encourages input from key stakeholders on establishing and maintaining clusters as well as your participation in PSTP's upcoming Call for Proposals, workshops and symposia.

Andrew Vallerand, Ph.D., is the Director of the Public Security Technical Program at Defence Research and Development Canada's Centre for Security Science in Ottawa. For more information on PSTP, please visit http://www.css.drdc-rddc.gc.ca/pstp/index-eng.asp or contact Dr. Vallerand – (613) 796-4765, andrew.vallerand@drdc-rddc.gc.ca. For details on the upcoming symposium in June 2008, please visit http://www.css.drdc-rddc.gc.ca/symposium/reg-insc/index-eng.asp.

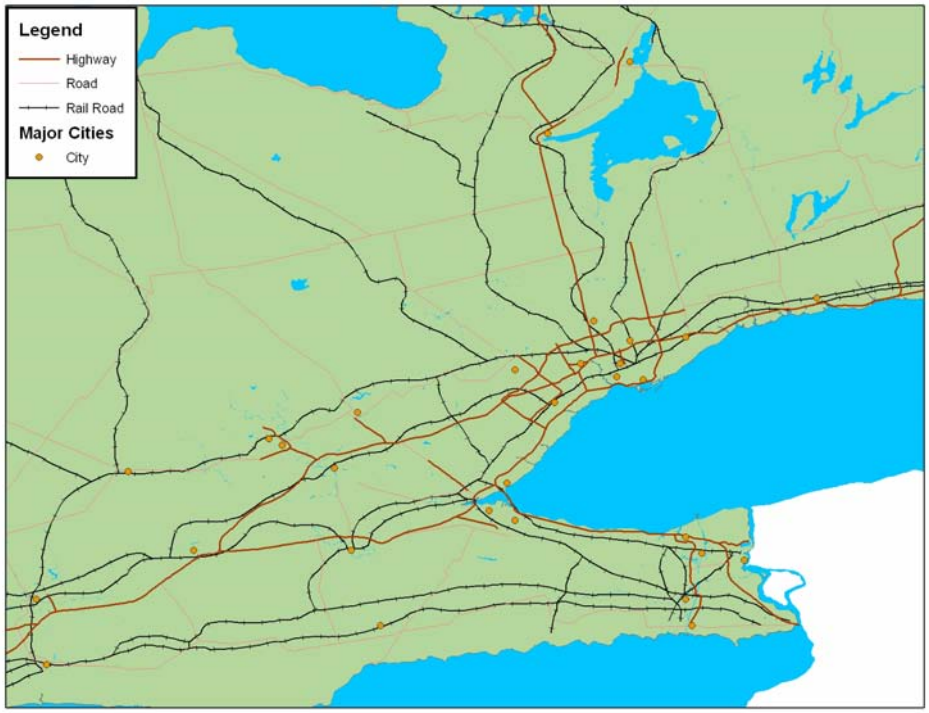


GEOMATICS and CIP:

A View from the Top

by Ronald Pelot

Spatial representations and analyses play a crucial and growing role in critical infrastructure protection. The increasing power of computers, the connectivity afforded by the internet, and the intensive effort to populate geographic databases with a wide range of elements and attributes have enabled effective use of Geographic Information Systems (GIS) for disaster management. Its evident prevalence in emergency response planning and execution has been mirrored to some extent in CIP planning, given the significant overlap in these spheres.



The power of GIS derives from its potential for rich layering of information, from basic data to complex spatial modeling outputs. In contrast with non-geographic decision-support systems, GIS can offer several benefits, with two key factors being paramount: visualization of the information, and location-based assessments. As a powerful communication tool between CIP decision-makers, maps are a very effective means for conveying a vast amount of information quickly while emphasizing subtle nuances which often cannot be communicated otherwise. This applies equally for strategic planning, such as simulating floods to assist with prioritizing preventative measures through land-use planning or new dikes; tactical planning for resource allocation to improve mitigation in areas of higher risk from certain threats; or operational situations during emergency response to critical infrastructure damage.

The power of GIS derives from its potential for **rich layering of information**, from basic data to complex spatial modeling outputs.

Primary data sets include basic information on the assets to be protected (location, identification), geographic variables of interest, and spatial representations of hazards or threats. The threat/hazard layers may be derived from historical information, such as typical hurricane corridors, or be created through simulation or expert-based scenario generation. Recent developments in the field involve populating some of the databases automatically through sensor-webs, which also serve for detection of developing threats and real-time tracking of some events.[1] While many primary data sets

[1] Abdalla, R., Ali, H. & Tao, V. (2006), "GIS-based Multidimensional Approach for Modeling Infrastructure Interdependency", in Lecture Notes in *Geoinformation and Cartography: Innovations in 3D Geo Information Systems*, Eds. Abdul-Rahman, A., Zlatanova, S. & Coors, V., Springer, pp. 295-305.

One important contribution is the ability to create dynamic simulations of events for better planning and protection.

are fairly comprehensive, challenges exist with respect to compatibility, sharing restrictions due to possible privacy violations or maintaining competitive advantage, and unauthorized access for nefarious purposes.

Famously, risk is a function of probability and consequence. Although ideally spatial CIP models would involve full-blown risk representations, the capacity to determine reliable probability and consequence measures is constrained. Many factors which influence probability and consequence are not easily quantified. Typically, these factors vary in time, space and perspective; the range of possible hazards also varies considerably. Nevertheless, most models include some of the elements of a risk evaluation. Thus, important attributes of the assets might include property value, local populations at risk (possibly with diurnal and/or seasonal variations), and links between infrastructure systems. More advanced risk aspects include vulnerability of assets to certain threats, likelihood of damage, consequences in terms of direct damage to the critical infrastructure, or consequent impacts to other systems. This latter issue encompasses the notion of interdependencies between critical infrastructures which, according to one popular taxonomy, can be classified into four types: physical, cyber, geographic, and logical.[2] Although geomatics has been used to conduct evaluations from each of these four perspectives, its principal contribution naturally lies in the geographic realm. Key spatial characteristics associated with the critical infrastructure assets themselves include proximity to each other (when relevant) which may reflect joint vulnerability to a single threat or collateral damage due to adjacency, proximity to other geographic features (such as a shoreline), and representations of the spatial impacts of interactions (such as power outage effects on water supply distribution).

Many more sophisticated geomatics functions have been developed for particular event types or contexts. One important contribution is the ability to create dynamic simulations of events for better planning and protection. Some span the entire time frame from the occurrence of the hazardous event to the evaluations of multiple consequences downstream. Others focus on a particular window of time, often either pre-initial impact (i.e. threat development) or post-event consequences.[3] The resiliency of critical systems depends on numerous factors, some of which have spatial characteristics. For example, redundancy is included in most distribution networks associated with utilities, information and transportation sectors (where alternative pathways are usually available), and geomatics serves to evaluate vulnerabilities and overall network reliability. To illustrate, a communications network that is broken at one location can usually reroute messages through different channels, so designers must evaluate which locations are more susceptible to damage, and how resilient the entire system is to diverse disruptions. Another research thrust in GIS modeling for disaster management involves resource allocation and response planning. Response resource layers in a GIS can be used to estimate reaction times to incidents or preparedness planning through scenario generation applying alternative critical infrastructure protection or response mechanisms.

In all cases, the ability to generate, evaluate and appreciate the complex spatial interactions yields significant benefits for CIP planning.[4]

Ronald Pelot, Ph.D., P.Eng., is a Professor of Industrial Engineering and the director for the Centre for Risk Management at Dalhousie University in Halifax, Nova Scotia. His twenty years of experience in risk management include spatial analysis for maritime safety and security modeling, and environmental risk analysis. For more information, please contact Dr. Pelot - (902) 494-6113, ronald.pelot@dal.ca.

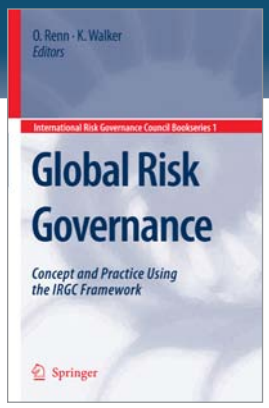
[2] Rinaldi, S., Peerenboom, J. & Kelly, T. (2001), "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, IEEE, pp. 11-25.

[3] Pederson, P., Dudenhoeffer, D., Hartley, S. & Permann, M. (2006), "Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research", *INL Technical Document*: INL/EXT-06-11464.

[4] Eveleigh, T.J., Mazzuchi, T.A. & Sarkani, S. (2006), "Systems engineering design and spatial modeling for improved natural hazard risk assessment", *Disaster Prevention and Management*, Vol. 15, No. 4, pp. 636-648.

BOOK Review

by M. Craig O'Blenis



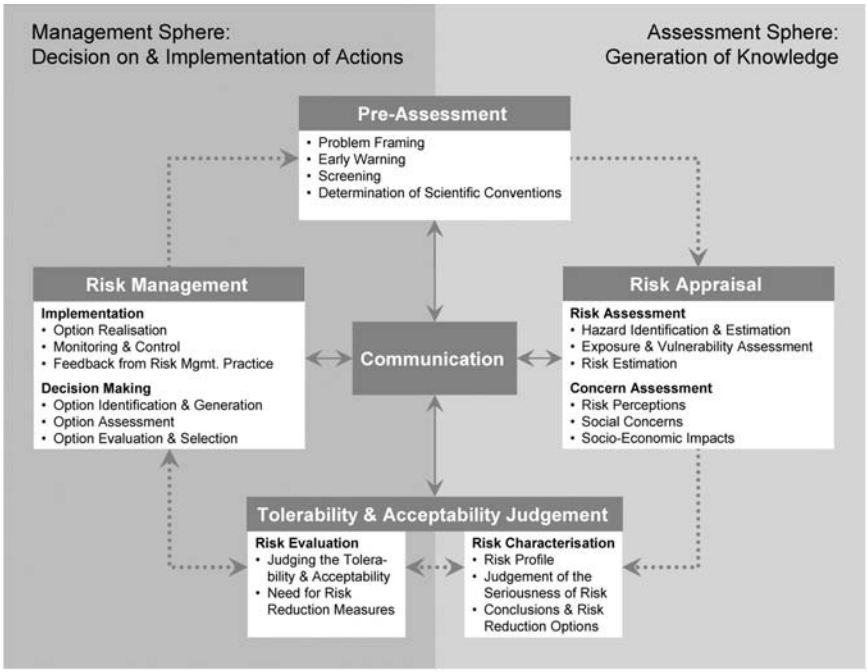
Global Risk Governance: Concept and Practice Using the IRGC Framework

Edited by Ortwin Renn and Katherine D. Walker, Springer, 2008.
ISBN: 978-1-4020-6798-3.

The International Risk Governance Council (IRGC) is an independent organization whose purpose is to help the understanding and management of emerging global risks that have impacts on human health and safety, the environment, the economy and society at large. IRGC focuses on emerging, systemic risks for which governance deficits exist and aims to provide recommendations for how policy makers can correct them.[1] The IRGC takes a broad, interdisciplinary approach; it draws specialists from practice and academe, and from natural sciences as well as social sciences.

In *Global Risk Governance: Concept and Practice Using the IRGC Framework*, Ortwin Renn[2] presents a risk management framework that aims to provide a comprehensive and transparent approach to managing physical risks with global or ubiquitous consequences. This framework is the result of extensive international consultation with risk managers and the academic community.

The framework has four stages beginning with *pre-assessment* where stakeholders and experts help decision makers frame risks. Here, managers increase institutional activity in risk by, for example, establishing agreed standards and early warning systems that identify questionable deviations from the norm. The second step is *risk appraisal*, which includes two phases: first, scientists estimate the consequences of a potential threat, and second, social scientists consider civil society's understanding of the risk. The third stage is *tolerability and acceptability judgement* where managers weigh the empirical evidence against different social values and perceptions. The final step is *risk management*. Typically, this step requires significant stakeholder involvement. The book notes that by including the public in the process, managers can increase transparency in decision-making and distribute the responsibility for risk reduction between governments and society. When risk managers are unable to reach a consensus, constant communication and transparent monitoring can often help stakeholders agree on provisional solutions. Given the nature of risk governance, the IRGC's framework is a recurring process as depicted in the accompanying figure.



IRGC Risk Governance Framework

Renn suggests that one of the most important risk policy issues is the treatment of different actors' risk perceptions. Availability and assessment biases, over- and under-estimation of risks, and risks spread over time (even over generations) challenge the traditional, straightforward risk calculations and projections. Renn argues for better integration of lay views with those of experts. On

[1] Taken from the IRGC vision statement (www.irgc.org).
[2] Renn and Walker are the editors of the book. Renn is the author of the chapter that introduces the framework.

the balance, he favours the latter; however, both have to be considered in order to generate stable risk-management solutions and a lasting sense of security.

The framework also includes clear definitions of key terms, including the distinction of different types of risks. The framework distinguishes, for instance, between risks that are highly complex; uncertain; or ambiguous. Complex risks are those which are difficult to quantify, largely because of the multitude of potential causal agents at work. Uncertain risks refer to a state of knowledge in which the likelihood of any adverse effect or the effects themselves cannot be described precisely even though the factors influencing the issues are identified. Ambiguous risks—perhaps the most contentious aspect of the book—give rise to several meaningful and legitimate interpretations of accepted risk assessment results.

Managers can rely on expert judgement when society agrees on the values underpinning a decision and the tolerability of the risk. When risk is considered complex, managers need an accepted method by which to compare available evidence. When risks are judged to be uncertain, Renn advocates a precautionary approach. When a risk is ambiguous, he suggests that a broad societal discourse will help overcome differences in values and perceptions.

The book has limitations. First, it is relatively new. While several chapters include very interesting case studies from around the world, the authors of these chapters in most instances have applied the framework in an after-the-fact approach. It will be important to see the impact that the framework will have when it is applied in a detailed and systematic way to new and emerging risks. This will take time. Second, its somewhat academic tone and style make it a little less accessible to a broader audience. Third and perhaps most importantly, the framework's strength can also be its weakness. While consultation is an important part of the process in a democratic society seeking stable risk management solutions, as Löfstedt and van Asselt as well as North note in their respective chapters, it is often difficult to build consensus, and therefore consultation can also be expensive and time consuming. Indeed, conducting the appropriate amount of consultation might be a bit more art than science. This is a significant challenge for most risk management processes; again, more time and research will suggest the extent to which the framework can accommodate multiple and competing views, and do so in an acceptably efficient manner.

For more information on the International Risk Governance Council's research on this and other policy files, please visit their website, www.irgc.org. Notably, the IRGC has recently published *Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures*, a copy of which is available on their website.

Craig O'Blenis is a recent graduate of Dalhousie University's Masters of Public Administration program. For more information on this article, please contact him at craig.oblenis@gmail.com

SEE PAGE 15 FOR REGISTRATION DETAILS

The Implications of Multi-Organizational Interdependence: A Dialogue about Critical Infrastructure Protection in Halifax

Critical infrastructure protection is the focus of increasing attention among governments and industry stakeholders with the recognition of our growing reliance on complex, interdependent and sometimes fragile systems. Failure in one system can have a cascading effect causing multiple, simultaneous failures.

Themes for the Workshop:

- Managing Risk and Interdependence
- Information Management and Change Management
- New CIP Standards and Regulations
- New Academic Research
- Best Practices from the Field

Who should attend? Those in the public and private sector who have responsibility for managing operational risks and mission-critical assets.

June 3rd, 2008 • 9 a.m. – 6 p.m.

Critical Infrastructure Protection in ONE Day? A Modest Proposal

Kevin Quigley sets up the upcoming workshop at Dalhousie

Anyone who thinks that interdependence is not the name of the game (fortunately) did not watch the Leafs this season: all excellent players in their own right but as a team, abysmal.

One might draw a parallel with critical infrastructure. Critical infrastructure depends on complex and interdependent systems. Failure in one system can have a cascading effect causing multiple, simultaneous failures. Consider the 2003 North American power outage: overgrown trees in Ohio helped trigger a power failure that affected 50 million people and cost the U.S. economy anywhere from $4 to 10 billion[1] — potentially more than the $8.5 billion that the U.S. government spent on its highly publicized and sometimes criticized Y2K preparations, in fact.

The problems are not merely technical. Many social, organizational and jurisdictional obstacles prevent successful Critical Infrastructure Protection (CIP).

The Goals for our June 3rd Workshop at Dalhousie

- Generate a dialogue about key interdependencies that exist in the region
- Examine the constraints and opportunities that shape our capacity to protect critical infrastructure
- Discuss best practices
- Consider future prospects for shared dialogue and collaboration on this subject

For most Western countries, critical infrastructure is owned and operated by a large number of organizations from both the public sector *and* the private sector. As I noted in the last edition of *The CIP Exchange*, corporate executives and their shareholders are sometimes reluctant to invest in CIP because its benefits are often indeterminate. They are also reluctant to disclose the vulnerabilities of their assets because of the risk to their organization's security, liability, reputation and share value. There is also a problem with trust. Industry executives worry that sensitive information shared with government may be used (surreptitiously) for reasons other than CIP. Government officials are equally reluctant to share sensitive information. Bureaucracies are hierarchical: accountability is bottom-up; outward accountability is not their strong card. Also, even well-intentioned information exchange in the appropriate context can quickly become 'leaked intelligence' and can bring about economic disaster or even human devastation on a massive scale. Finally, overlapping responsibilities between different organizational units and levels of government can obscure accountability and complicate planning. In short, despite its acknowledged importance, CIP is an area in which it is difficult to achieve meaningful cooperation and transparency.

There is also reason to work together, however. In many instances the infrastructure is only as strong as its 'weakest link.' Cascading failures do not discriminate; and therefore there is a shared interest in cooperation. Business continuity and recovery planning, redundancies, risk communication and change management, for example, are subjects that offer opportunities for an exchange of ideas and best practices.

The goal of the CIP initiative at Dalhousie is to create opportunities for citizens, industry, NGOs and governments to engage with questions and ideas concerning the management of Canada's critical assets, exploring technical as well as social and economic opportunities and constraints. We seek to enrich the discussion about the complexity of the infrastructure and the holistic approaches necessary to make it more secure and resilient for the benefit of all who depend on it.

Universities across many industrialized countries are playing an important supporting role in helping to generate this kind of dialogue. George Mason University in Virginia has perhaps the most noted CIP program. Others are joining in the act, however. Cass Sun-

[1] US-Canada Power System Outage Task Force (2004), *Final Report*, available at: https://reports.energy.gov/.

stein—one of our feature interviews—is leaving the University of Chicago for Harvard Law School to start a new program in risk regulation. The news release notes that "the Program on Risk Regulation at Harvard will focus on how law and policy deal with the central hazards of the 21st century." The program will focus on terrorism, climate change, occupational safety, infectious diseases, natural disasters, and other low-probability, high-consequence events. European Union Framework 7—the EU's latest research strategy—identifies CIP as an area in which greater international research and collaboration are required. Carleton, too, will join the fray; it plans to offer a new Masters of Infrastructure Protection and International Security (MIPIS).

At first glance, the goals for the June 3rd workshop seem to be a stretch: in a networked society, critical infrastructure is ubiquitous, an integral part of day-to-day life. Can one possibly wrap one's arms around it in a day? Absolutely not. And for that reason we have a more modest agenda in mind. We would like to generate a discussion about some of the matters we have raised in this article. Both locally and across the country, many people are already having these discussions. We hope that the workshop will generate deeper discussion, and perhaps allow others to join in and learn from the debate. We are particularly interested in creating a cross-sectoral and cross-jurisdictional space in which participants can access and share diverse and expert perspectives on protecting the critical infrastructure. We hope it is successful, and will stimulate further discussions in the future.

The Framework for the Workshop

We have elected to use Hood, Rothstein and Baldwin's (2001) Risk Regulation Regime framework to guide our discussion about CIP on June 3rd. Hood *et al* is sufficiently flexible in that it casts a wide net; the authors hypothesize that *context* shapes the manner in which risk is regulated. There are three elements that they use to explore 'context': the technical nature of the risk, including the role of law and insurance; the public's and media's opinions about the risk; and the way power and influence are concentrated in organized groups.

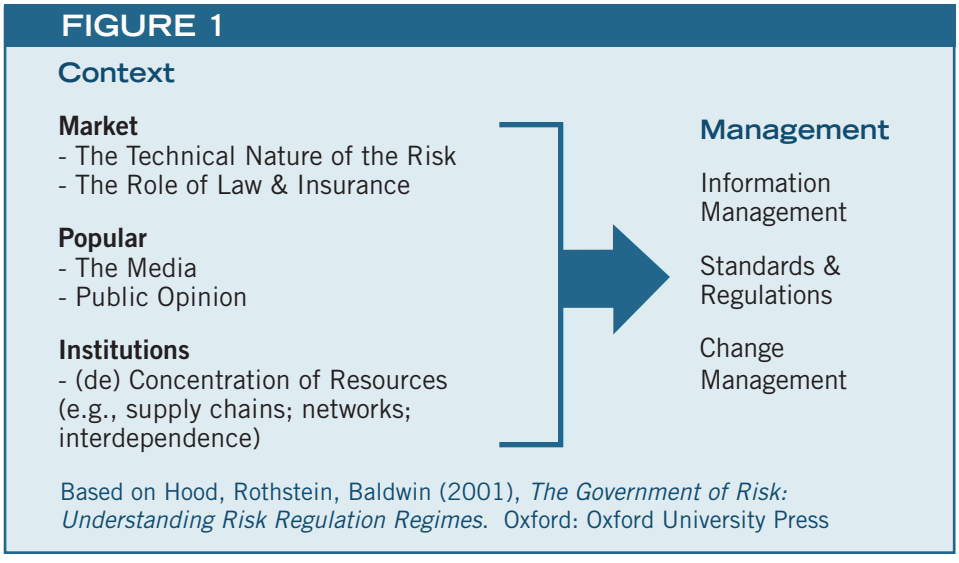
Hood *et al* use these separate pressures to examine the extent to which each of them explains our management responses to risk. In particular, they use three elements to characterize management: information management; standards; and changing behavior. Figure 1 outlines the approach for the workshop.

As a result of adopting this perspective, the workshop has been designed to allow for a broad and divergent discussion within the key sub-topics of management and context. We hope the format—plenary, breakout sessions and keynotes, organized along the lines of the Hood framework—coupled with an audience drawn from academia as well as the public and private sectors, respectively, will lend itself to a lively exchange of ideas on this subject.

If you have an interest in and/or responsbility for managing operational risks and mission-critical assets, either in the public sector or private sector, we encourage you and your colleagues to attend. You will find a registration form attached to the back of this newsletter.

Dr. Kevin Quigley is Assistant Professor at the School of Public Administration at Dalhousie University as well as a co-investigator in the CIP Initiative at the Faculty of Management. Comments are welcome and can be addressed to Dr. Quigley at kevin.quigley@dal.ca.

FIGURE 1



Based on Hood, Rothstein, Baldwin (2001), *The Government of Risk: Understanding Risk Regulation Regimes.* Oxford: Oxford University Press

This project is a collaboration between the Faculty of Management's School of Public Administration and the RBC Centre for Risk Management. Financial support from the Canada School of Public Service to conduct this work is gratefully acknowledged. The views expressed in this publication are not necessarily those of the Canada School of Public Service or of the Government of Canada.

Sponsored by:

Tuesday June 3 2008
9AM – 6PM

Dalhousie University
Rowe Building
6100 University Ave.
Halifax NS B3H 3J5

The Implications of Multi-Organizational Interdependence:
A Dialogue about Critical Infrastructure Protection in Halifax

Registration Form

Name _____
Company _____
Address _____
_____
Telephone _____ Fax _____
E-mail _____
Special Dietary Requirements _____

Tickets are $125 + $16.25 (HST) = $141.25
Please make cheque payable to "School of Public Administration" and mail to Cecilia Macdonald, Dalhousie School of Public Administration, 6100 University Ave. Halifax, NS B3H 3J5 or pay by credit card and fax to 902-494-7023

☐ AMEX
☐ VISA
☐ MasterCard

Name on Card _____
Number _____ Expiry_____
Signature_____

Hosted by

DALHOUSIE UNIVERSITY
Inspiring Minds

In partnership with

Canada School of Public Service
École de la fonction publique du Canada

For more information consult our website at **www.cip.management.dal.ca** or e-mail us at **cip@dal.ca** or contact Dave Smart at **david.smart@dal.ca**