THE CIP EXCHANGE

A forum for sharing views and information about critical infrastructure protection FALL 2007

Balancing Security and Efficiency

Dalhousie University hosts panel on critical infrastructure protection

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

CONTENTS

1 Balancing Security and Efficiency
3 Interview with Margaret Bloodworth, National Security Advisor to the Prime Minister
5 Interview with Peter Nicol, President of CH2MHILL Canada
7 Emergency Services in N.S.
8 CIP Research at UBC
9 Canada's New *Emergency Management Act*
11 Civil Protection Research in Norway
12 Review: *Seeds of Disaster*
13 Editorial

EDITORIAL

Editor: Kevin Quigley

Managing Editor: Jennifer Mark

Copy Editor: Julie Davies

Design: Dalhousie Design Services, Roxanna Boers, Designer

Research Assistant: Stewart Fraser

Additional Thanks: Ron Pelot, Director, RBC Centre for Risk Management

Fingerprint technology seems so archaic after listening to Gord Helm describe a vascular scan system used at the Port of Halifax. The system reads blood flowing through the veins in the back of your hand and then stores the information on a security card chip for identity verification purposes. Helm, Manager of Port Security and Marine Operations for the Port of Halifax, was a panelist on October 30th in Dalhousie University's first public event in the Critical Infrastructure Protection Initiative. The event attracted a diverse audience of over 60 attendees representing private industry, all levels of the public sector and the academic community. Chaired by Dr. Kevin Quigley with the School of Public Administration, the panel discussion focused on the challenges of sharing sensitive information across organizations responsible for protecting critical infrastructure.

One of Helm's greatest concerns is striking a balance between security and efficiency, since the Port of Halifax plays a key role in local, national and continental economies. The Port acts as a strategic hub linking Halifax to Chicago in the North American transportation network. This is a complex operation involving cargo infrastructure, power generation, tourism and the Navy with the potential for significant repercussions in the event of a natural or manmade disaster.

Helm explains the complexity of port security before a full house at Dalhousie.

Yates takes questions from the audience.

Helm has leveraged his own naval experience to develop an information network linking Port stakeholders in an effort to improve safety and security without sacrificing operational efficiency.

Information that is collected in isolation may seem insignificant; however, important patterns can emerge when information is shared in real-time and viewed in conjunction with information from other sources. Helm gave the hypothetical example of someone in a van trying to access a restricted area while claiming to be lost. On its own, this may seem inconsequential. However, by relaying a record of this incident along with security camera footage to other organizations at the Port, a later attempt to penetrate a secure area at another facility in the same way is recognized as a threat and handled quickly and effectively. In order to create and distribute what he calls a "fused picture," Helm described how the Port Security Command and Control System acts as a nerve centre that collects and analyzes information submitted voluntarily by various organizations via a fibre optic network.

A fundamental problem for Helm is getting organizations to agree to share information. For competitive reasons, private companies do not want to disclose information. For legislative and policy reasons, government organizations *cannot* disclose information. Helm's challenge is to create a viable system that provides a value-added network so organizations see the benefits inherent in being a part of such an alliance. According to Helm, this integration of public and private collaboration is a unique situation in North America.


The audience included representatives from academia and the public and private sectors.

Helm was joined by fellow panelist Carl Yates, General Manager of the Halifax Regional Water Commission (HRWC), who faces similar challenges in sharing information among utilities. On one hand, he believes that many organizations are in a state of denial and haven't even started the process of implementing security measures, and he hopes that it doesn't take a serious incident for this to change. At the same time, there are utilities that take security seriously, but are reluctant to report incidents due to concerns around negative publicity or exposure to future liability.

Since the events of 9/11, Yates has noted a cultural shift among many of the owners and operators of critical infrastructure as heightened security measures replace an earlier complacency among water utilities. Where once public tours were a common occurrence, access is now restricted by numerous security measures including fences, locks, alarms, electronic access control and CCTV surveillance. Ironically, despite the importance of ensuring the safety of drinking water in HRM as well as the provision of fire protection services, water utilities were not considered a part of critical infrastructure protection in Canada prior to 9/11.

In leading HRWC through this shift in mindset, Yates has participated in measures such as a Water Information Sharing and Analysis Centre (ISAC) pilot project to create a framework for sharing information between American utilities and five of the largest water utilities in Canada, including that of Halifax. The HRWC's membership with the Canadian Water and Wastewater Association (CWWA) also ensures that Yates receives the latest information originating from the Department of Homeland Security and the Integrated Threat Assessment Centre. In establishing a secure, web-based database on incidents and responses and by working closely with the CWWA Water Protection Information Committee, the HRWC can access and communicate the latest security information. As Yates notes, "Sharing information is a tactical response to a security strategy." HRWC is also a member of the American Waterworks Association Research Foundation (AwwaRF) which ensures access to leading-edge training programs.

Professor Elaine Toms, who holds the Canada Research Chair in Management Informatics at Dalhousie University, was in the audience. She feels that the panelists underscored the need for strategic thinking in terms of how security-based information is managed and the complexities inherent in how we share that information. "This presents an interesting dichotomy," she says. "On the one hand, we need stringent controls to protect critical infrastructure like our water supply, as indicated by Yates. However, we also need a viable framework to facilitate collaborative information sharing. As Helm highlighted with regard to Port security, this has immediate and direct economic consequences. Ultimately, this dichotomy has significant ramifications for policy and legislative decisions around security."

To download a video of the panel event, please visit our webpage at www.cip.management.dal.ca.

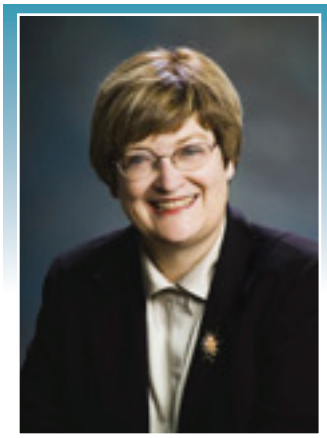
Stewart Fraser is currently completing his MBA with the Faculty of Management at Dalhousie University. For additional information on this article, please contact him via email, stewart.fraser@dal.ca.

Interview with

Margaret Bloodworth

National Security Advisor to the Prime Minister

Balance and Resilience



Margaret Bloodworth has held the position of Deputy Minister for Transport Canada, the Department of National Defence, and Public Safety and Emergency Preparedness Canada. In May 2006, Ms. Bloodworth was appointed to the position of Associate Secretary to the Cabinet, and on October 10th, 2006, she assumed the responsibility of National Security Advisor to the Prime Minister. Margaret Bloodworth is a respected authority on national security issues.

KQ: What is the government's medium-term goal for CIP?

MB: Our goal is probably best described as resilience, a goal which has both proactive and reactive aspects to it. Ideally, we do our best to prevent infrastructure failures from occurring in the first place. By the same token, we are never going to be able to mitigate every risk: that is not an achievable goal. So we have to be able to respond effectively when situations occur. And our response has to include everyone who manages critical infrastructure, whether in the public sector, private sector or NGOs.

So, where are we? We have learned through experience. Y2K, 9/11, the 2003 blackout—these events have taught us how to better prepare our critical infrastructure to withstand failures. Are we resilient enough? I'm not sure anyone in my position would say "yes" to that question. I think there are specific areas where we could improve; for example, one area is information sharing among those who are responsible for critical infrastructure. That is one of the most difficult issues we face, largely because the information is often sensitive; people are understandably cautious about sharing information concerning infrastructure vulnerabilities.

KQ: Where does the government wish to be three years from now on this issue?

MB: In three years, I'd like to think that we will have formalized more information-sharing networks that stakeholders will use to exchange useful information. This is one of the reasons why I find your project very interesting. It has the potential to generate not just one network, but a number of these kinds of networks.

KQ: Is the public sufficiently engaged in the CIP debate?

MB: Recently, I think the government has made progress in raising public awareness in this and related areas. The public education campaign, *72 hours: Is your family prepared?*, for instance, suggests reasonable precautions people can take to reduce the impact of an emergency. In this respect, families and communities are part of our critical infrastructure. Rural communities in Canada already excel in this way by reaching out to help family and neighbours when situations arise. On 9/11, thousands of people were grounded in Goose Bay and Gander, and the local population opened their doors and invited them into their homes. No one told them to do it; they just responded naturally. Of course, the Red Cross and the government became involved, but much of the response was driven by the communities themselves. Ultimately, however, our goal should be for all Canadians to be resilient and prepared.

> Our goal is probably best described as resilience, a goal which has both proactive and reactive aspects to it.

KQ: What is the Canadian government doing to engage other jurisdictions on the subject of CIP? What remains to be done?

MB: There are three broad jurisdictions to consider: relationships within Canada; the Canada-U.S. relationship; and, Canada's relationship with the rest of the world. First, within Canada, there is no question that we are in a stronger position than we were five or six years ago. There is now an established federal/provincial/territorial structure involving all levels, including

ministers, that meets regularly, considers all sorts of emergency management issues, shares concerns and priorities, and works jointly to address them.

Second, with so many systems tied together, the Canada-U.S. relationship is a very important one for both countries. The Canadian and American governments are committed to enhancing information sharing and to conducting joint vulnerability assessments and protection exercises. However, Public Safety Canada and the Department of Homeland Security are still relatively new organizations and we need to strengthen our mutual capacity. We need to build up corporate memory and expertise. On a scale of one to ten, we're probably at six or seven right now. And we must get to ten.

> The private sector is not looking for the government to fix the problem. They want the government to be a catalyst, to play a leadership role in bringing together people from across all parts of the private sector.

Third, and finally, on the international front, most of the work has happened at the sectoral level, such as through the International Civil Aviation Organization (ICAO) and the International Maritime Organization (IMO), for example. That said, we have also worked with allies like the U.S., the U.K., Australia and New Zealand in areas such as preventing cyber attacks, for example. However, different countries have progressed at different rates, and therefore, this remains an area where there is more work to be done.

KQ: How is the government engaging the private sector and how effective has its commitment been to date?

MB: The private sector owns the vast majority of critical infrastructure. They are aware of the interdependencies between sectors and the vulnerabilities that can result from those interdependencies. There are numerous examples of key industries making significant headway in the area of CIP. The Government of Canada has key partnerships with the private sector. For approximately three years now, we have had an information-sharing agreement with Microsoft, for example. In addition to having expertise that we could never replicate, Microsoft is fundamental with regard to our own cyberinfrastructure. Clearly, this is an important relationship.

In general, the private sector is not looking for the government to fix the problem. They want the government to be a catalyst, to play a leadership role in bringing together people from across all parts of the private sector. That is what we are trying to achieve.

KQ: How is the government balancing transparency with the need for secure and trusted information exchange in the area of CIP?

MB: That is always an issue in national security. To create good public policy, I believe we need openness in government. On the other hand, we don't want to announce our vulnerabilities. That is not in the public's interest. So the challenge becomes finding that balance between being as open as possible about policy while protecting key information that might cause vulnerability in the critical infrastructure. The new *Emergency Management Act* attempts to maintain that balance by protecting information shared by the private sector with government. The private sector—and I think with some justification—is worried about sharing information about its vulnerabilities. So this legislation provides protection to prevent this information from becoming public. Industry associations see this as key in striking that balance.

> To create good public policy, I believe we need openness in government... So the challenge becomes finding that balance between being as open as possible about policy while protecting key information that might cause vulnerability in the critical infrastructure.

Kevin Quigley interviewed Margaret Bloodworth on August 21st in her office in Ottawa. This text has been edited for publication.

CIP Workshop: Interdependencies in Atlantic Canada

Hosted at Dalhousie by the School of Public Administration and the RBC Centre for Risk Management
Date: June 3rd, 2008
Email cip@dal.ca for more information.

Vision and the Hidden Infrastructure

Peter Nicol, President of CH2MHILL Canada, offers his views on Canada's critical infrastructure

CH2MHILL Canada has been providing engineering services in Canada for over 85 years. It has 21 offices and 1,500 staff in Canada. It is part of CH2MHILL, an international company with 23,000 staff in over 30 countries. It specializes in infrastructure projects in numerous sectors, including energy, water, transportation, power, manufacturing and communications. Peter Nicol has been the president of CH2MHILL Canada since August 2006. He is a professional engineer with over 27 years of experience in project design and leadership.

KQ: Where do you think the most significant vulnerabilities are in Canada's critical infrastructure?

PN: The hidden, underground infrastructure, such as sewer collection and water distribution systems. I would also include foundations for roads and bridges. Unfortunately, these infrastructures are out of sight and, therefore, too often out of mind.

> At present, in Canada, infrastructure decisions are too often made in an *ad hoc* manner.

KQ: What can organizations or sectors in general do to address these vulnerabilities?

PN: The sector-based approach is the right approach. And from our perspective, looking at a risk-based approach for funding decisions is essential. You have to identify and prioritize risks and then develop a rational asset management program based on those risk assessments. We recognize there is a limited amount of money and that there are an ever increasing number of challenges. A risk-based approach will help to use limited funds most effectively.

KQ: What role should governments play to help ensure the resilience of critical infrastructure?

PN: We certainly believe that government needs to play an active role. Government must set standards or guidelines so that when sectors (or even multiple sectors) are tackling infrastructure challenges, there is an agreement on the approach we have to take. Government guidelines can facilitate agreement among stakeholders.

KQ: Is it helpful for government to facilitate the exchange of sensitive information between organizations on the subject of critical infrastructure vulnerabilities?

PN: We think there are a variety of ways that governments can reach out. They can sponsor workgroups or strategic workshops. They can solicit ideas from industry associations. They can also act as think tanks with this information, which can drive changes and create solutions.

KQ: How does CIP practice in Canada compare with CIP practice in the U.S.?

PN: The process is more mature in the U.S. and the U.S. government is certainly more active. The U.S. has implemented a formal process through GASB 34.[1] (Canada's PSAB 3150[2] is not quite there yet.) There are also more federal funding initiatives for roads and bridges, for instance. At the same time the infrastructure in some U.S. markets is often older than the infrastructure in Canada. That's not to say there isn't a lot of work to do here. It's a matter of getting your arms around it—figuring out where your highest priorities are. At present, in Canada, infrastructure decisions are too often made in an *ad hoc* manner: on a case by case or project by project basis rather than from a broader, integrated perspective. There are some interesting exceptions, however, such as the governments in Alberta and British Columbia deciding to reinvest a percentage of gas taxes in infrastructure renewal. We need more initiatives like that.

KQ: Where do you expect the CIP discussion or debate to be three years from now?

[1] Government Accounting Standards Board, Statement 34. For more information, please visit GASB's website at www.gasb.org/.
[2] For more information, please see the Public Sector Accounting Board website at www.cica.ca/index.cfm/ci_id/225/la_id/1.htm.

Long-term vision has to be included in the infrastructure plan.

PN: Life cycle costing and asset management will be critical. I think as PSAB 3150 is implemented, it will drive a lot of activity—as GASB 34 did in the U.S. There will be a greater emphasis on risk-based approaches and risk profiling. There will also be greater emphasis on quality service provision rather than simply looking at who's coming in with the lowest bid. Low-cost service provision gives us exactly what we pay for. We need to think about public-private *partnerships* with a focus on quality. I think there will also be growth in incentives for "green" infrastructure.

KQ: Are there jurisdictional issues that create barriers when working with government?

PN: I think every level is interested in doing the right thing, but it isn't clear how they work together to implement a project. If something is funded by one level of government alone, it's much easier to implement. When you have several levels of government involved, we seem to have many more objectives to meet. We need to have a clearer understanding of what it is that we're trying to accomplish collectively, what is a "win" for everybody, so to speak? The more jurisdictions that get involved, the cloudier it gets.

KQ: What aspects of working with public sector clients can be particularly promising? What aspects can be particularly challenging?

PN: Public sector clients have embraced sustainability. They have truly increased activity in that regard and are doing some really interesting things across the country. On the challenging side, most of this infrastructure has a life span of 20 to 100 years. Most politicians have only three or four years before they face an election. It takes some really strong leadership to agree to some of these projects because politicians' terms in office could be long over before the community really sees the value of the asset that the politicians agreed to build.

Infrastructure is designed and implemented with future use in mind. New bridges are not designed for the number of traffic paths that are used *today*. Typically they are designed to anticipate the growth patterns of the community. Long-term vision has to be included in the infrastructure plan.

KQ: "Best practices" is one way to communicate infrastructure protection. What about the slightly darker side of CIP—when there are vulnerabilities?

Public- and private-sector entities want to understand their vulnerabilities... However they are less willing to share that information with others.

What can government do to facilitate a discussion about infrastructure vulnerabilities? Is it realistic to think private industry is going to disclose information about its vulnerabilities?

PN: What we've seen in the marketplace is that public- and private-sector entities want to understand their vulnerabilities and implement vulnerability plans. However, they are less willing to share that information with others. It seems to come down to liability issues. If they identify vulnerabilities and don't fix them quickly enough, they are concerned they will be held liable. Typically information about vulnerabilities is for private use only. There are more workshops on vulnerability, but it is unclear that this will lead to greater disclosure of potentially sensitive information. The exchange of this information will likely be through the service providers—the organizations that serve the marketplace and work in critical infrastructure. They are going to be the holders of some of the lessons learned and will bring what they know and what they are learning to infrastructure projects.

Kevin Quigley interviewed Peter Nicol on Monday, October 22nd in Peter Nicol's office in Toronto. The text has been edited for publication. If you would like to hear the entire interview, you may download it as an audio file from our webpage at www.cip.management.dal.ca.

CALL FOR SUBMISSIONS

We invite contributions on the subject of critical infrastructure protection for future editions of *The CIP Exchange*. Perspectives from practitioners and academics alike are welcome, and while the initiative has a Canadian focus, we appreciate international contributions. We are particularly interested in highlighting new research and practices in the field. Op-ed pieces are also welcome. Articles should be 600-1000 words. Please contact the editor, Kevin Quigley, at cip@dal.ca for further information.

If you have any comments about this edition of *The CIP Exchange,* please email them to the editor.

The Province of Nova Scotia and the Canadian Red Cross: Working Collaboratively for Emergency Social Services

by Erin Edmundson, Suzanne Gélinas and Joanne Sullivan

On the evening of September 2nd, 1998, Swissair Flight 111 crashed into the Atlantic Ocean off Peggy's Cove *en route* from New York to Geneva. As the Province of Nova Scotia scrambled to action in its first major emergency response since taking over the provision of social services from its municipalities, the Canadian Red Cross proved to be an invaluable ally in coordinating all support organizations and volunteers from its central command centre in Halifax. Impressed by their experience and expertise, the Province eventually formalized this partnership through a contract between the Department of Community Services (DCS) and the Canadian Red Cross for the provision of emergency social services (ESS) in Nova Scotia.

> "The link between policy and practice in disaster mitigation needs to be established at the local level."
>
> *Louise Comfort, University of Pittsburgh*

Disaster mitigation is an integral component of critical infrastructure protection and according to Professor Louise Comfort at the University of Pittsburgh's School of Public and International Affairs, "The link between policy and practice in disaster mitigation needs to be established at the local level."[1] In partnering with the Canadian Red Cross, the Province effectively strikes this balance by harnessing the capacity of a highly respected non-governmental organization that specializes in emergency preparedness, disaster response and management while still retaining overall control, a key concern when government outsources such a vital service.

While there had been no specific arrangement for the Red Cross to respond to emergencies prior to this agreement, historically the organization has been active in emergency response services in Nova Scotia since the devastating Halifax Explosion in 1917. Originally signed in 2000 (and renewed annually), this contract is not without its challenges, but both the DCS and the Red Cross believe that the benefits far outweigh these concerns and a formal contract with a sole emergency service provider ensures clear roles and responsibilities, evaluations and results.

For the Province, this collaboration is a highly cost-effective method of channeling financial support into a non-profit volunteer organization that specializes in emergency responses which, by their very nature, require extreme dedication of time and human resources. This allows their own staff to focus on more appropriate day-to-day government functions while eliminating duplication of services. In a less tangible manner, the Province also benefits from alignment with the Red Cross as an international symbol of respect and credibility in disaster management. Given that emergency situations are highly disruptive and unsettling, this emblem can instill a sense of comfort and trust among victims who are seeking assistance.

Red Cross volunteers distribute supplies.

According to John Webb, Director of Emergency Social Services with the DCS, a key concern with shifting responsibility for ESS provision to the Red Cross is the loss of control, since clearly the Red Cross needs some level of autonomy to develop its own strategies and operational techniques based on its expertise and experience. However, both organizations recognize the importance of maintaining strong relationships and open communication channels to ensure that response capacities are at required levels. Additionally, the contract is careful to outline the responsibilities of both

[1] L.K. Comfort, et al. "Reframing disaster policy: The global evolution of vulnerable communities." *Environmental Hazards*, June 1999, 1:1, 42-43.

the Canadian Red Cross and the DCS while stipulating that the Minister of Community Services has the final say and authority in the provision of emergency social services in Nova Scotia.

From the perspective of the Red Cross, there is the obvious benefit of stable and predictable funding. According to Ancel Langille, a Field Associate for the Halifax area, the arrangement has also opened doors for the Red Cross to engage in strategic planning for emergency services with the DCS and the Emergency Management Office (EMO). In terms of evaluation and results, the contract specifies that the Red Cross must develop an Annual Report highlighting emergency social services that have been provided in the previous year in addition to conducting an annual policy and operational review to ensure compliance with DCS policy. This review was particularly useful in assessing the challenges faced by the Red Cross during Hurricane Juan in September 2003. As a result, the Red Cross was required by the DCS to increase volunteer training and revamp its volunteer call out to improve future responses. The inherent problem with such disasters is that they are difficult to predict, and the success of these new measures remains unknown until the next emergency situation.

According to Langille, Nova Scotia is the only province to have this legally binding, contractual arrangement with the Red Cross to provide a complete range of emergency social services including food, clothing, lodging, registration & inquiry, personal services and shelter management. Far from being simply a contract, it is hoped that establishing and formally recognizing the relationship between the DCS and the Red Cross will encourage an ongoing commitment to citizen-centred emergency social services.

Erin Edmundson, Suzanne Gélinas and Joanne Sullivan are recent graduates of Dalhousie University's Masters of Public Administration program.

For more information on this article, please contact Erin Edmundson, Internal Auditor with the Internal Audit and Risk Management Centre, (902) 424-3997 or edmunde@gov.ns.ca.

UBC's Disaster Research Lab Focuses on Infrastructure and Resilience

by Stephanie Chang & Tim McDaniels

Secure, resilient communities require critical infrastructure systems that deliver key services (e.g., electric power and water) even in extreme events such as storms, earthquakes, floods or other disasters. Yet urban infrastructure systems are increasingly under pressure from both growing demand and difficulties in expanding capacity, resulting in infrastructure system failures that occur with increasing frequency. However, as highlighted by the aftermath of Hurricane Katrina, if an extreme event occurs and causes a series of interconnected infrastructure failures, the effects can be devastating as even limited power outages can disrupt water systems, transportation, and hospitals.

A team of researchers at the University of British Columbia (UBC) has been working on the issue of how best to keep services flowing through critical infrastructures in disaster situations. Stephanie Chang, Associate Professor and Canada Research Chair at the School of Community and Regional Planning (SCARP) and the Institute for Resources, the Environment and Sustainability (IRES), is leading the Disaster Preparedness Research Centre and its associated lab. Together with Dr. Tim McDaniels, they lead a group of outstanding students from SCARP and IRES as well as from the engineering and law faculties at UBC in research activities. Two major research projects on critical infrastructure interdependencies have been pursued over the last few years.

One project is supported by the National Science Foundation in the U.S. through a grant to the University of Washington and addresses what the group calls "IFIs" or *infrastructure failure interdependencies*. This work takes an empirical look at what actually happens in situations where one kind of infrastructure failure leads to failures in other systems by studying interactions that have occurred in real disasters such as the Quebec ice storm in 1998 or three hurricanes in Florida in 2004. In particular, this study focuses on which types of IFIs cause the greatest societal impacts. A series of papers highlighting

the results of this research have been published in the J*ournal of Infrastructure Systems*, *Natural Hazards* and other forums. One of the latest papers is an attempt to characterize factors that contribute to resilience in all types of infrastructure systems, the decision contexts before and after a disaster and when decisions can best be made to foster resilience.

A second grant has led to an unusual, larger scale project which attempts to understand the factors affecting regional infrastructure resilience in the context of a specific region with an emphasis on how IFIs can be considered in infrastructure decision-making. Supported by Infrastructure Canada's Knowledge, Outreach and Awareness program, the project has several components which include developing an earthquake scenario for Greater Vancouver and interviews with all the major infrastructure providers regarding the function of their systems in this event. A workshop follows to clarify interdependencies and set priorities regarding regional infrastructure resilience. A website has been developed to support and disseminate findings from this study (www.chs.ubc.ca/dprc_koa/).

Other research projects conducted through UBC's Disaster Research Lab include a paper published in *The Electricity Journal* by Colleen Brown, formerly a practicing lawyer, outlining the legal liability of infrastructure providers when a system fails. Another more recent project by Sarah Wilmot developed a decision support framework for setting priorities as part of hospital earthquake mitigation efforts.

UBC's Disaster Research Lab welcomes keen and talented students to work on similar projects that seek to understand and enhance regional disaster resilience. For more information, please contact Dr. Chang, Associate Professor - (604) 827-5054, stephanie.chang@ubc.ca, or Dr. McDaniels, Professor - (604) 822-9288, timmcd@interchange.ubc.ca, at the University of British Columbia's School of Community and Regional Planning (SCARP) and the Institute for Resources, the Environment and Sustainability (IRES).

Canada's New Emergency Management Act: Implications for Information Sharing

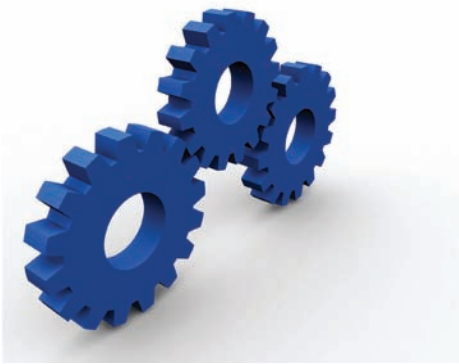
by Public Safety Canada

Critical infrastructure is broad in scope and touches virtually all aspects of life - from food and water, to energy and finance. Safeguarding these essential assets and services requires an integrated, horizontal approach across federal departments and with our partners in the provinces and territories and in the private sector.

Emergency Management Act

On August 3, 2007, the federal government took a big step forward with the coming into force of the *Emergency Management Act*. Bringing greater accountability to emergency management at the federal level, the new Act modernizes the Government's approach by aligning federal roles and responsibilities with today's threat environment and complementing existing provincial/territorial approaches to emergency management and critical infrastructure protection.

As part of this new legislation, federal ministers are responsible for identifying risks within their areas of responsibility, including risks to critical infrastructure. Moreover, each department or agency is required to develop emergency plans to address these risks. Each department is responsible for maintaining, testing, and exercising these emergency management plans according to the policies and programs established by the Minister of Public Safety.



On an international scale, the Act recognizes that the impacts of attacks or disruptions can cascade across borders and sectors. The *Emergency Management Act* enables the Minister of Public Safety, in consultation with the Minister of Foreign Affairs, to coordinate Canada's response to an emergency in

The *Emergency Management Act* includes consequential amendments to the *Access to Information Act* that protect specific critical infrastructure/emergency management information shared in confidence.

the United States, as well as develop joint plans and initiatives.

Information Sharing

Collaboration and information sharing are longstanding traditions connecting all levels of government in Canada and the private sector which translates into a common commitment to enhance the security, prosperity and quality of life in Canada. Government of Canada information-sharing practices related to critical infrastructure protection are based on the principles articulated in the *Access to Information Act* (ATIA) which include the public's right to access information held by the Government of Canada along with specific exceptions to that right. The exceptions in the ATIA are similar to information-sharing legislation in each of the provinces and territories.

Building on Canada's current system of safeguards, the *Emergency Management Act* includes consequential amendments to the ATIA that protect specific critical infrastructure/emergency management information shared in confidence by private sector owners and operators of Canada's critical infrastructure. This type of information will enable the Government of Canada to develop comprehensive emergency management plans, mitigation and preparedness measures, improve warning capabilities and develop better defences and responses, thus helping to bring emergency management into the 21st century. The ATIA also exempts from disclosure any information that is considered important to national security. Exemptions from disclosure for reasons of national security and public safety also exist under provincial jurisdictions.

To improve two-way information sharing, the Government of Canada will also need to demonstrate value-added and provide the private sector with accurate information in a timely manner. To improve the quality and timeliness of information products, Public Safety Canada will (in partnership with the Integrated Threat Assessment Centre and the Royal Canadian Mounted Police) work directly with industry experts to produce more targeted information, in a Canadian context, that owners/operators can use to protect their assets and essential services.

"The *Emergency Management Act* will greatly enhance the partnership that already exists between industry and the Government of Canada, as the protection accorded to information provided by industry to government will allow for a far greater depth of collaboration," said Mr. Francis Bradley, Vice President of the Canadian Electricity Association.

National Strategy for Critical Infrastructure Protection

To ensure a higher level of readiness and effective information sharing, Canadians want all levels of government working together to protect critical infrastructure. Canada's national approach is two-fold. First, the draft *National Strategy for Critical Infrastructure Protection* will set out the overarching concepts relevant to all critical infrastructure sectors and jurisdictions. Aligning the activities and challenges of each of the critical infrastructure sectors and each jurisdiction within a coherent roadmap is fundamental to identifying risks, reducing vulnerabilities, addressing interdependencies and effectively responding to disruptions. Moving forward with this collective approach, the *National Strategy* will serve as the basis for enhanced collaboration between all levels of government and the private sector and, as such, will remain 'evergreen'.

To keep pace with the rapidly evolving threat environment, an ongoing state of renewal is required. Therefore, the second element of Canada's national approach is the development of a flexible Action Plan that builds on the central themes of the *National Strategy*: sustainable partnerships with all levels of government and the private sector, improved information sharing and protection, and a commitment to all-hazards risk management. This Action Plan will be updated on an iterative basis to enable partners to anticipate new risks and adopt new best practices.

Together, the *National Strategy for Critical Infrastructure Protection* and supporting Action Plan, in addition to the *Emergency Management Act*, will establish a collective approach that will be used to set national priorities, goals and requirements for critical infrastructure protection. This collective approach will enable funding and resources to be applied in the most effective manner to reduce vulnerabilities, mitigate threats, and minimize the consequences of attacks and disruptions.

For more information, please contact Suki Wong, Director, Critical Infrastructure Policy, 269 Laurier Avenue West, Ottawa, Ontario, K1A 0P8, (613) 991-3583.

New Research Initiative in Norway:
Multilevel Governance and Civil Protection

by Per Laegreid

Multilevel governance can complicate the issues surrounding civil protection by presenting significant organizational challenges. Norway is a typical example of this complexity, having undergone comprehensive change and reform at local, regional and national levels of government over the past fifteen years. Until now, no study has focused on using organizational theory and a political science approach to civil protection. It is our view that the organization of public safety can be a particularly useful subject with which to explore issues of multilevel governance, especially the interplay between vertical and horizontal coordination, specialization by function and territory and the effectiveness of public-private partnerships.

Recent government policies have expanded the number of organizations involved in ensuring the public's safety. Volunteer organizations such as Norwegian People's Aid have always played a central role in rescue services. However, increased structural devolution, the establishment of state-owned companies and privatization have increased significantly the number of entities that play a role in civil protection.

Coordination is a fundamental challenge in this complex dynamic. Vertical coordination relates to sector-based coordination between levels of administration, state and municipality, or between central and local government. Horizontal coordination refers to coordination between policy areas or sectors at the same level, for example, between civil protection policy and the various sector policies. In matters of civil security, functions and responsibilities are dispersed both horizontally and vertically and there is often little coherence in the relevant policies. Both forms of coordination are needed to manage civil protection. For example, vertical coordination is normally found centrally within the state and focuses on the coordination of resources. Horizontal coordination is more often found at the local or regional level where it focuses on the coordination of activities. The coordination between public authorities and volunteer organizations —such as with the Red Cross—is often characterized by both a vertical and a horizontal dimension. In this project, we are studying how these coordination mechanisms interact. In particular, we will consider whether or not the structure of such mechanisms has changed over time in matters of civil protection, and if so, what the consequences of these changes have been.

One reason that this interplay between different coordination mechanisms can change is due to the variety of approaches to specialization selected at central, regional and local levels. Generally, increased specialization generates a stronger need for coordination. In an organizational hierarchy, there may be one specialization principle at one level, and another at a higher or lower level, which can impact steering and coordination decisions. A central question in this project is whether key organizations in the state and municipal sectors should have common approaches to specialization or if indeed diverse approaches to specialization across these organizations and jurisdictions would result in more effective civil protection.

The tension between integration, administration and control on one hand, and flexibility, autonomy and self-government on the other, is an integral part of our project. Throughout our study, we plan to examine policy documents and survey civil servants employed at different levels of government. Our surveys will focus on administrators' understanding of responsibilities, tasks, skills, capacity, resources, resource use, priorities, expectations and motivation. We will also include questions about networks, contacts, coordination and administrative relations.

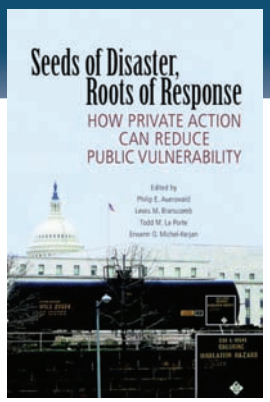
Through specific public safety case studies, we can consider the implications of events on subsequent internal control systems and supervision. We will also survey the general public and employees in the Norwegian central administration, soliciting their views of coordination in crisis preparedness and the authorities' management and prevention of crises.

This project is associated with the Department of Administration and Organisation Theory and the Rokkan Centre at the University of Bergen. We also plan to exchange experiences with a broader Nordic and international network. Our three-year project (2007-2010) will bring together these highly-respected research communities based on the recognition that the most important challenges in the Norwegian system of governance will be found at the interface between the administrative levels and sectors.

Professor Per Laegreid is with the Department of Administration and Organization Theory at the University of Bergen. He welcomes any comments or questions that you may have concerning this research project. Please contact him via email, per.lagreid@aorg.uib.no.

BOOK Review

by Tom Woods



Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability

by Philip E. Auerswald, Lewis M. Branscomb, Todd M. La Porte, and Erwann O. Michel-Kerjan, Cambridge University Press, 2006. ISBN 0-521-68572-9.

Nowhere has the discussion over critical infrastructure protection been more intense than in the United States. Since 9/11, there has been exponential growth of popular debate, policy initiatives, legislation and academic research. Indeed, the creation of the Department of Homeland Security is one of the most significant acts of the current administration; it will have a lasting impact on how the U.S. government engages with industry and citizens on issues of national security.

In *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, academics Philip E. Auerswald, Lewis M. Branscomb, Todd M. La Porte, and Erwann O. Michel-Kerjan bring together leading scholars working on CIP to analyze how to address public concerns about security when the vast majority of critical infrastructure remains in private hands. The authors identify a dilemma with which governments must engage. Organizations operating in markets seek to cut costs in order to remain efficient and gain advantage over competitors. While eliminating redundancies can cut costs and in so doing, satisfy shareholders, it can also make systems more vulnerable to failure. This is particularly problematic when organizations are interdependent. When one organization in the supply chain eliminates operational redundancies in the name of efficiency, the entire supply chain becomes potentially more vulnerable. There are other issues as well. Somewhat cynically, one might also note that low probability / high consequence failures that occur in critical infrastructure create ideal conditions for free-riders. In these sectors, private companies can underinvest in business continuity planning knowing the government will be forced to prop them up in a disaster due to the critical nature of their service. In short, private interest may conflict with the public good in the CIP debate. Ultimately, this creates a situation where the United States, despite its power, remains vulnerable to serious system failures. What measures can be taken to address this? As implied in the title, this book arrives at the consensus that encouraging private action is the key to success.

By any definition, critical infrastructure is remarkable in its breadth. Of the sectors that the Department of Homeland Security have identified as critical, each one is incredibly complex with huge scope for potential research. This diversity highlights a wide variety of problems ranging from different and potentially incompatible theoretical approaches for managing disaster response and strengthening organizational behavior to inconsistencies in the insurance industry and strategies to improve compliance and information sharing.

In covering such a wide range of material, *Seeds of Disaster, Roots of Response* provides an insightful look at the two distinct approaches to managing the vulnerabilities of critical infrastructure. Attempts can be made either to protect infrastructure from attack or to strengthen its capacity to respond once it has been attacked. While popular political efforts have tended to focus on the first approach, in a world where systems are increasingly interconnected, the second approach may be more effective over the long term. Indeed, when the effect of one attack cascades into many other areas, disaster mitigation may be the only practical option.

Although largely successful in their analysis, the authors focus primarily on the American context, frequently drawing examples from the September 11 attacks, the 2003 power failure and Hurricane Katrina. While the authors examine these cases from different angles, there is still considerable overlap between chapters. And although these three events are extremely important and informative, it would also be refreshing to see the researchers consider international developments more fully. Finally, due to the scope of the problems inherent in CIP, inevitably some areas are covered perhaps a bit more superficially than one would have hoped.

Solving the riddle of critical infrastructure protection will necessarily be complicated. The authors believe that the private sector can provide security, but guidance and cooperation from government is essential. A more structured environment with new policies is needed to create incentives for private businesses to act. Ultimately, governments must display initiative in convincing the private sector to play a larger, more effective role in protecting critical infrastructure. While efforts have been made, more must be done if government is to fulfill the responsibility to protect its citizens.

Tom Woods is a recent graduate of Dalhousie University's Masters of Public Administration program. For more information on this article, please contact him at woods.thomas@gmail.com.

Context and CIP

Editorial by Kevin Quigley

The goal of Dalhousie's CIP Initiative is to create opportunities for citizens, industry, NGOs and governments to engage with questions and ideas concerning the management of Canada's critical assets. It is our view that CIP occurs in a particular context. One of the primary interests of the project is to explore this context, examining technical as well as social, political and economic opportunities and constraints.

In Canada—as in many other Western countries—governments are taking steps to ensure the country's critical infrastructure is managed more effectively. There have been formal institutional changes, such as the expansion of the roles and responsibilities of Public Safety Canada and provincial emergency management operations. There has also been a strengthening of ministerial leadership and responsibility, as articulated in the Public Safety Canada article on the new *Emergency Management Act*. Governments are trying to collaborate more. Memoranda of understanding between jurisdictions and joint emergency planning exercises are more common. The Canadian federal government is also looking to work more closely with the private sector, which owns the vast majority of the critical infrastructure, with an eye to managing vulnerabilities proactively.

> Much like the creation of the EPA altered the debate about the environment, the creation of the Department of Homeland Security will change the dialogue about domestic security and the context in which it occurs.

Previous studies of risk management caution, however, that bringing discipline to this multi-sectoral dynamic will be difficult. In their comparative study of risk management in nine different policy areas in the UK, Christopher Hood, Henry Rothstein and Robert Baldwin[1] conclude that the size, structure and style of risk regulation by government vary considerably across policy areas and jurisdictions.

The authors argue that the variation can be explained by contextual factors: different pressures influence policy areas and jurisdictions differently. They explore the impact of context by testing three separate hypotheses. The first hypothesis, the *Market Failure Hypothesis*, examines the government's intervention as a necessary one, given the inability of the market to manage the risk effectively without such intervention.

A competitive market context does not always lend itself readily to proactive CIP. Corporate executives and their shareholders—sensitive to market pressures—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, share value and public image. Moreover, there is a problem with trust. Industry executives worry that sensitive information shared with government may be used (surreptitiously) for reasons other than CIP. Also, insurance coverage in this area can be expensive, and sometimes unreliable.

Traditionally, industries could try their luck; if they chose to take risks and failed, then the market would punish them accordingly. Because organizations that manage critical infrastructure are increasingly interdependent, however, individual decisions to underspend on CIP and/or not disclose CIP-related information is now a risk for the entire critical infrastructure and all those who depend on it. This is indeed a market failure to which government will undoubtedly continue to respond one way or another.

The market context is not the only relevant context in the discussion about

[1] Hood, C., Rothstein, H. and Baldwin, R. (2001), *The Government of Risk: Understanding Risk Regulation Regimes.* Oxford: Oxford University Press.

CIP, however. The second hypothesis, the *Opinion Responsive Hypothesis*, examines the extent to which risk regulation is a response to the preferences of civil society. Here they consider the role of the media and popular opinion in influencing government response. CIP media coverage often goes in fits and starts: it peaks in a crisis and then falls away. The infrastructure failures we learn about most often are spectacular failures, as we saw in the recent bridge collapses in Montreal and Minneapolis. The insatiable appetite of 24/7 media coverage influences not only the way civil societies understand the problem, but also who, if anyone, is to blame. This pressure generates considerable incentive for short-sighted reactions and blame-avoidance strategies among key stakeholders.

The third hypothesis, the *Interest Group Hypothesis*, takes a well-trodden path in political science and examines the role of organized interest groups and professional communities in shaping risk regulation through lobbying power or institutionalized expertise, or both. This last hypothesis is particularly relevant in recent CIP policy initiatives. Most Western governments have engaged with critical sectors over CIP issues, but each sector has its unique characteristics. As Carl Yates, General Manager of the Halifax Region Water Commission (HRWC) noted in the panel event, the HRWC is a monopoly and is therefore potentially in a better position to share information across organizations than organizations in competitive, multi-organizational, multi-sectoral settings, such as those in the Port of Halifax.

No one hypothesis holds the answer to why governments respond the way they do. But by testing each hypothesis, we come closer to understanding the issue in the round. We gain useful insights to the multiple pressures that potentially influence policy decisions about risk, each with its own merits and potential drawbacks.

Governments are not merely subject to these contextual pressures, however. They can apply pressure themselves. Governments not only respond to the law, through legislative bodies they make the law. Most Western governments have sought and received the backing of their national legislatures as they have expanded their intentions for national CIP strategies. Governments also engage civil society through the media; they don't simply react to a 24/7 media. Indeed, their capacity to strike an appropriate balance between transparency and discretion will be important in earning popular approval in this area.

Finally, with respect to interest group interaction, the government has the capacity to facilitate the exchange of information about vulnerabilities and best practices across policy areas in ways that other organizations cannot. In most Westminster countries at least, government is the one constant in all sector-level fora. Certainly some sectors will be easier to work with than others. Its success will depend partly on its capacity to share meaningful information efficiently. This means negotiating legal constraints deftly, yes, but it also means overcoming turf wars within governments and trust problems with industry. Government must also ensure that the data exchanged are compatible. This is easier said than done. Different sectors and jurisdictions have different ways of gathering information.

Voluntary fora—such as the ones most governments propose for CIP initiatives—derive their influence through persuasion, trust or membership self-interest. They are often tenuous arrangements. Information is filtered through biased industry associations. When things go wrong participants drop out. They threaten to sue if their security lapses will be disclosed. The governments risk losing their capacity to act as arbiters for the sector, knowing that by actively participating in these fora their authority diminishes as they become merely interested participants at a round-table.

Governments must be sensitive to all contextual pressures, but not captured by any one in particular. Striking the balance between these inherent tensions will not be easy. By the same token the problems are not likely to go away. The Department of Homeland Security (DHS) is here to stay. Public Safety Canada is also likely to remain. They were borne of a particular context and to fulfill a need. They are now part of the context. Much like the creation of the EPA altered the debate about the environment, the creation of the Department of Homeland Security will change the dialogue about domestic security and the context in which it occurs. The CIP Initiative at Dalhousie seeks to contribute to and enrich this dialogue by helping to examine this context.

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.

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: