THE CIP EXCHANGE

Workshop Edition

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

Raising their Game

Ken Button from George Mason University discusses what economics can bring to our understanding of CIP

by Julie Davies, Julia McCarthy and Kevin Quigley

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

CONTENTS

EDITORIAL

Editor: Kevin Quigley

Assistant Editors: Julie Davies and Julia McCarthy

Design: Dalhousie Design Services, Roxanna Boers, Designer

Additional Thanks: Ron Pelot (Industrial Engineering), Patrick McDougall and Craig O'Blenis (School of Public Administration)

Many traditional approaches to risk management are ineffective in the context of terrorism. Game theory, however, can help guide our reasoning and assist us in developing appropriate strategies for dealing with terrorists.

These were among the observations of Ken Button, author of over 100 books and Director of both the Center for Transportation Policy, Operations and Logistics and the Center For Aerospace Policy Research in the School of Public Policy at George Mason University.

Button was the keynote speaker at Dalhousie's Critical Infrastructure Protection (CIP) workshop held last June that brought together over 60 participants from the public, private and academic sectors to spark dialogue on the challenges in CIP.

To understand why traditional risk calculations are ineffective in the context of terrorism, Button distinguishes between 'safety' and 'security.' He describes safety in the context of an inherently dangerous event in which the likelihood of the event occurring is generally understood and agreed upon. Button cites earthquakes in certain regions as an example. In contrast, he describes 'security' in the context of uncertain and unpredictable events such as terrorism. Because the probability cannot be determined for the latter with any degree of confidence, traditional *probability multiplied by consequence* risk calculations become impossible.

He was also skeptical of cost-benefit analyses (CBAs). CBAs are useful for smaller projects, he acknowledged; however, major incidents affect prices throughout the entire economy, which make CBAs difficult to apply.

Button is confident though that economics has much to contribute to our understanding of CIP. Game theory is vital, Button noted. It helps

Ken Button, keynote speaker

Health Communication Seminar on November 18th. Please see pages 15-16

Button addresses over 60 participants from more than 20 organizations

us to anticipate how terrorists are likely to behave. In addition to Game theory, he also notes input-output analysis, which reflects how damage in one sector has economic implications on other sectors, can also be used in macro studies of infrastructure protection. Other economic valuation techniques, specifically those involving 'implied value for life,' valuing time, econometric modeling and forecasting can also prove useful in CIP.

Button's address initiated considerable discussion. In the Q & A that followed one participant wondered if Game theory could be applied not only to understanding terrorists' strategies but also to understanding the behaviour of collaborators in supply chains with a shared interest in protecting themselves from disruptions brought about by acts of terror. Perhaps more controversially, participants also discussed the tactic of deliberately limiting the release of information about threats to the public as a way of bolstering confidence in the system.

It was a thought-provoking start to the CIP Workshop's daylong event of presentations, one that underlined the continuing need for cooperation and information-sharing and the inherent challenges of the contemporary security context.

To download Professor Button's talk in its entirety, please visit the audio and visual files of the CIP website: www.cip.management.dal.ca

Fences and Neighbours: Partnerships Necessary and Constrained in CIP

Workshop panelists tackle compliance, politics and jurisdictional issues

By Julie Davies

While greater collaboration across organizations on CIP is desirable, financial pressures and jurisdictional issues constrain this collaboration. That was the resounding note struck by the panel discussion that concluded the CIP Workshop at Dalhousie University on June 3rd.

John Moloney, Business Development Manager for Ultra Electronics Maritime Systems, stressed the importance of resiliency and funding. In enabling recovery after incidents occur, Moloney sees industry as the "arms and legs" of academia and government. While industry excels at commercialization, its "biggest challenge is dollars" especially in Nova Scotia where small and medium-sized enterprises are so common and profit margins much thinner. Moloney emphasized until funding is in place, compliance with CIP standards will continue to be difficult for smaller enterprises. He would like to see a better process for engaging private industry through government funding, investment and cost-sharing in CIP.

...until funding is in place, compliance with CIP standards will continue to be difficult for smaller enterprises.

Marie Sassine agreed with the need for greater engagement of public, private and academic sectors but noted the balancing act that often confronts governments. Sassine, Associate Assistant Deputy Minister, Safety & Security, Transport Canada cited the trade-off in the concept of corridors and gateways in the transportation sector as an example. While promising economically, the concept is problematic for national security. She noted other challenges. Transport Canada has no authority in urban and rail transit, for instance. These are high-risk targets requiring jurisdictional cooperation. Echoing Button's earlier distinction between 'safety' and 'security' (see previous article on Button), Sassine indicated people with responsibility in safety often have responsibility in security also. This has advantages, according to Sassine. Transport Canada can leverage its longstanding relations in the safety community to develop stronger partnerships in the security community.

Jez Littlewood, Director for the Centre for Intelligence and Security Studies at Carleton University, argued "that politics affects everything" in CIP, particularly when it comes to resource allocation and the justification of government intervention in markets. He shared Moloney's concerns about the challenges that face industry in complying with government regulations and sees tough decisions ahead in enforcement. For Littlewood, the biggest challenge for academics is as fundamental as defining the role they should play: should they be trainers, researchers? Littlewood indicated it would be beneficial for academics to examine (successful) case studies in this area, such as the 2010 Olympics and US homeland security post 9/11, to determine what works and why.

...the number of lives lost on September 11th was one-eighth of those lost annually in car accidents....

Littlewood also commented on the role of popular perceptions of risk and their impact on government risk management decisions, which was picked up again in the discussion that followed. Participants discussed how we make decisions about which risks we will manage. One participant noted, for instance, the number of lives lost on September 11th was one-eighth of those lost annually in car accidents in the U.S. Participants also questioned whether all the security investments since 9/11 had really changed anything or if such investments have merely served to create a superficial "cloak of security."

To download the panel discussion in its entirety, please visit the audio and visual files of the CIP website: www.cip.management.dal.ca


John Moloney, Ultra Electronics


Marie Sassine, Transport Canada

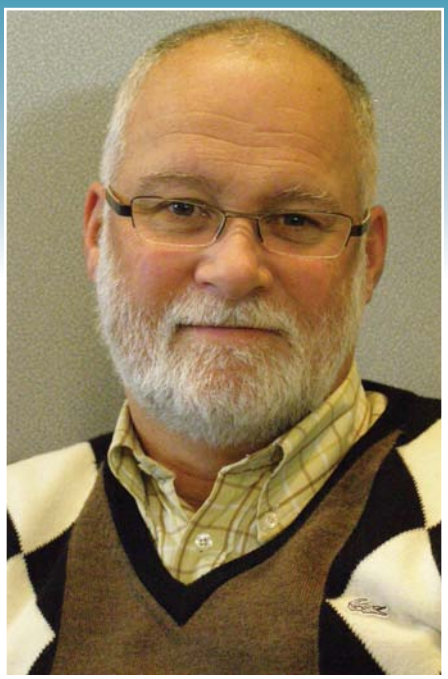

Jez Littlewood, Carleton University

Interview with
Daniel Lavoie

Public Safety Canada

Partners in Time

Public Safety Canada seeks partnerships in its new strategy and action plan



Daniel Lavoie, Emergency Management and National Security Branch, PSC

Earlier this year Public Safety Canada released its draft document *Working Towards a National Strategy and Action Plan for Critical Infrastructure* and solicited comments on it from members of critical infrastructure (CI) sectors. The Emergency Management and National Security Branch played a lead role in developing the strategy. Daniel Lavoie is the Acting Associate Assistant Deputy Minister at the branch. He spoke with Kevin Quigley by telephone on September 25.

KQ: Public Safety Canada (PSC) is five years old. Has the department successfully defined and operationalized its role?

DL: The department of Public Safety has evolved significantly since it came into being in December 2003. The Department's mandate is to protect the safety and security of Canadians. This includes emergency management, national security, border security, corrections, and national law enforcement. It is a diverse mandate and touches on the lives of Canadians across the country. We have defined our role by providing leadership and direction on all these issues. One of the best examples of this leadership is the *Emergency Management Act (EMA)*, which came into force in August 2007. The new EMA is perhaps the most significant achievement in the move towards modernizing emergency management in Canada. It is a relatively brief document but it gives the Minister a clear mandate to exercise national leadership in preparing for and responding to emergencies, including in the area of CI. This is significant - we now have a tool that outlines roles and responsibilities. Now we have to act on it. Using the EMA as a guide, we are engaging the provinces, the municipalities and the private sector on the issue of critical infrastructure.

KQ: How will the measures outlined in *Working towards a National Strategy and Action Plan for Critical Infrastructure (Plan)* improve the security and safety of Canadians in a tangible way?

DL: The *Plan* is a model for partnership—between the Government of Canada and owners and operators of the CI and the provincial and territorial governments. The document highlights how we want to approach these partnerships: based on sector profiles, risk assessments, work plans and exercises. We hope very quickly to have various sectors of the CI better equipped to identify, protect and react to threats with even greater effectiveness.

> "...we now have a tool that **outlines roles** and responsibilities. Now we have to act on it."

KQ: According to PSC's Canadian Disaster Database, the ratio of natural disasters to conflict disasters, which include acts of terrorism, is approximately 40:1. This ratio has been relatively stable since the end of the Second World War. How

is this reality reflected in current CIP planning in the Government of Canada?

DL: We have a lot of connections and interdependencies in society today. As a result, society needs to be ready to address all sorts of problems. In terms of protecting critical infrastructure, we know we must be prepared for contingencies of any sort. The importance of critical infrastructure and the interdependencies involved requires an overarching approach that is responsive and flexible enough to meet the demands of changing circumstances and evolving threats, natural or otherwise. Like many other Western countries, we are developing an *all-hazards* approach. The challenge is to develop it and make it work. Prevention planning, response and recovery—all that has to be brought together in a system that allows us to operate no matter what the emergency.

KQ: How does the new *Plan* address the needs and vulnerabilities of owners and operators of small and medium-sized enterprises (SMEs)?

DL: Small and medium-sized enterprises are major contributors to our economy. They rely on critical infrastructure in providing goods and services to Canadians. We are currently focusing on the larger infrastructure–those systems that would have the greatest impact on Canadians were they to fail: financial systems, transportation, communications and information technologies, etc. This is the canvas on which SMEs operate. In the medium term and building on the progress of the sector networks, as described in the *Plan*, I can see us working with SMEs, and providing guidance on the types of risks that exist and help them with developing emergency management plans.

> "Business continuity has a commercial benefit, certainly; but there is also social responsibility…."

KQ: The *Plan* emphasizes the role information-sharing plays in making the CI more resilient. Will the government use statutory instruments to make business continuity planning mandatory and/or specific financial incentives to encourage business continuity planning among owners and operators of the CI?

DL: I don't believe that additional legislation is necessarily the solution. We are developing an approach at the sector and cross-sector levels that has not been there before. Sector-level groups will facilitate information exchanges in key sectors—banking, petroleum, telecommunications, for instance. It will be a learning process. For example, at present we share information on different threats with CI owners and operators. With the *National Strategy and Action Plan*, that information will be more targeted and based on the information requirements of CI owners and operators themselves. Likewise, the EMA will provide the necessary safeguards to allow stakeholders to share information in confidence. Together with the provinces and the private sector we will create a much better security picture. We are confident we can achieve our desired goals by working in partnership and developing trust, not through forced legislative requirements.

KQ: How will the *Plan* manage the tension between security/safety and prosperity/efficiency?

DL: In the western world, safety and security are increasingly linked to prosperity and efficiency. When safety and security are not part of the day-to-day reality of ordinary citizens, chances are there is no democracy or that free enterprise is not working. Secure critical infrastructure is at the heart of our economy and our social prosperity.

Owners and operators of critical infrastructure know that people will still rely on their services whether somebody purposely makes a breach in a critical system or whether there is failure due to a storm or an earthquake. Business continuity has a commercial benefit, certainly; but there is also social responsibility to ensure that the infrastructure remains active.

What we're trying to do is develop a model for partnership based on information-sharing amongst the stakeholders in the various sectors. We will tell the owners and operators of CI about risks, and can work on the interdependencies with the cross-sector groups. First and foremost, however, owners and operators of CI know how their own businesses work and must be able to work on and develop their own plans.

The document *Working Towards a National Strategy and Action Plan for Critical Infrastructure* can be downloaded from the Public Safety Canada website: http://www.publicsafety.gc.ca/prg/em/cip/strat-part1-eng.aspx

The text of this interview has been edited for publication.

THE WORKSHOP BREAKOUT SESSIONS

By Kevin Quigley

The intention of the June 3rd workshop at Dalhousie was to bring together representatives from the public, private and academic sectors to facilitate a far-reaching discussion about the challenges of CIP.

We elected to use Hood, Rothstein and Baldwin's (2001) Risk Regulation Regime framework to guide our discussion. (See figure 1 on next page.) After Professor Button's keynote address in the morning, we held three breakout sessions, one for each aspect of management. In the afternoon we had another three sessions, one for each contextual element. Note, we deviated from the Hood *et al* framework somewhat. We did not organize a breakout session explicitly on the contextual issue of media and public opinion, due largely to time and capacity constraints. We ended the day with a panel event, which attempted to address some of the overarching issues and articulate a way forward on some of the key challenges.

We used a variation of the Chatham House Rule for the breakout sessions. The Chatham House Rule can be defined this way: "When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed." I note it was a variation of the Rule because each session started with one, two or three brief presentations from experts in the field. In the pages that follow we have identified these presenters and attributed their comments to them. Comments coming from the other participants in the breakout sessions – the audience – were noted by our note-takers but not attributed. We felt that by affording anonymity to the audience we would encourage a more free-flowing discussion. Participants were informed of the (somewhat liberal) use of the Chatham House Rule at the beginning of the day.

Following the event, note-takers wrote summaries of the discussions. Note-takers and I agreed upon the text. In certain cases we also discussed the content with breakout session chairs. The articles that follow are the result of this work. We regret any omissions that participants may feel that we have made.

Many topics came up in a variety of ways across sessions. I offer three themes in particular that struck me and include tensions that we may wish to consider further.

Standards and Compliance

Participants discussed how to ensure that the systems that underpinned CI met appropriate standards. Participants showed ambivalence here. How would these standards be developed? Who would enforce them and how? Who would pay for it?

On the carrot side, people suggested that the government offer financial incentives to businesses to develop business continuity plans or at a minimum a more efficient method to deal with industry on some key issues. There was particular reference to small and medium-sized enterprises and municipalities, which have particular needs. On the stick side, some suggested that legislative authority must back standards otherwise owners and operators of CI will not follow them. Some suggested more aggressive public reporting on the state of CI might prompt owners and operators to act.

There are a few tensions that will have to be managed here. One wonders how

To obtain a free CD of the workshop please contact Dolene Lapointe (dolene.lapointe@dal.ca)

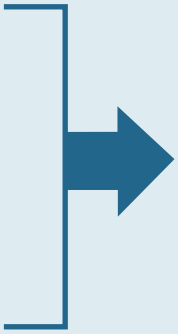
FIGURE 1

Context

Market
- The Technical Nature of the Risk
- The Role of Law & Insurance

Popular
- The Media
- Public Opinion

Institutions
- (de) Concentration of Resources (e.g., supply chains; networks; interdependence)



Management

Information Management

Standards & Regulations

Change Management

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

effective government would be if it seemed to tread on others' turf because, first, they may not have the authority, and secondly (and more importantly), it is unlikely to be helpful: organizations often know better how to protect their own organizations. The federal government is trying to articulate clearer standards and accountability through the new *Emergency Management Act* (EMA) and its new *National Strategy and Action Plan (Plan)*, which, among other things, encourages behaviour change largely through developing opportunities for sensitive information-exchange and cooperation.

Trust and Transparency Paradox

Academics have noted that trust is an under-researched topic; the term tends to be used ambiguously. Most agree that trust is a multi-dimensional concept that reflects the interaction of values, attitudes and socio-cultural references. Researchers have noted that 'open communication' is a prerequisite to organizational trust. Open communication can encompass practices such as free data sharing, inclusive decision-making and collaborative working.

> ...levels of disclosure can be effective in bringing about change; they can also bring about clearer accountability.

This also poses a challenge. The government's *Plan* looks to develop trusted relationships with key CI partners in order to facilitate the exchange of sensitive information. On the one hand, literature suggests that transparency is a prerequisite to this trust. On the other hand, too much transparency might make owners and operators of the CI nervous about disclosing information about vulnerabilities.

Sound judgment will be required in achieving the appropriate balance. What information should be disclosed? To whom, by whom and how? What information should be made available to the public and what is an appropriate method to disclose this information?

Transparency can be a powerful tool. As Cirtwell notes in his presentation, levels of disclosure can be effective in bringing about change; they can also bring about clearer accountability.

Complexity and Risk Management

Many discussed the complexity of the issue: the numerous stakeholders with formal responsibilities in this area as well as the myriad of complex technologies that underpin the systems. Accountability and expertise become diffuse. Reliable information can also run in short supply. The EMA and the *Plan* are efforts by the federal government at addressing a significant challenge: how should those with ownership and responsibility for CI coordinate their actions? Equally important is the question, what, in particular, requires coordination?

Few are under any illusion that this task will be easy. Risk management is often neglected as a study and an investment. It can seem like a drain on resources; and no one ever knows how much is too much. (Unfortunately, you only know when it's too little.) Still, these are extremely important questions, especially given the concessions in transparency that are likely. A strong focus on risk management process is a good place to start.

In closing let me thank everyone for participating in the workshop and offering their views. We hope all participants found the event rewarding.

Kevin Quigley is an Assistant Professor at Dalhousie University's School of Public Administration and a co-investigator of the CIP Initiative.

THE BREAKOUT SESSIONS

Session 1: Information Management

By Craig O'Blenis

PRESENTERS:

Mark Pryce
Director, Rogers Communications Inc., and Chair, Canadian Telecommunications Emergency Preparedness Association

Susan Topping
Emergency Planning Manager, Aliant and Vice-Chair, Canadian Telecommunications Emergency Preparedness Association

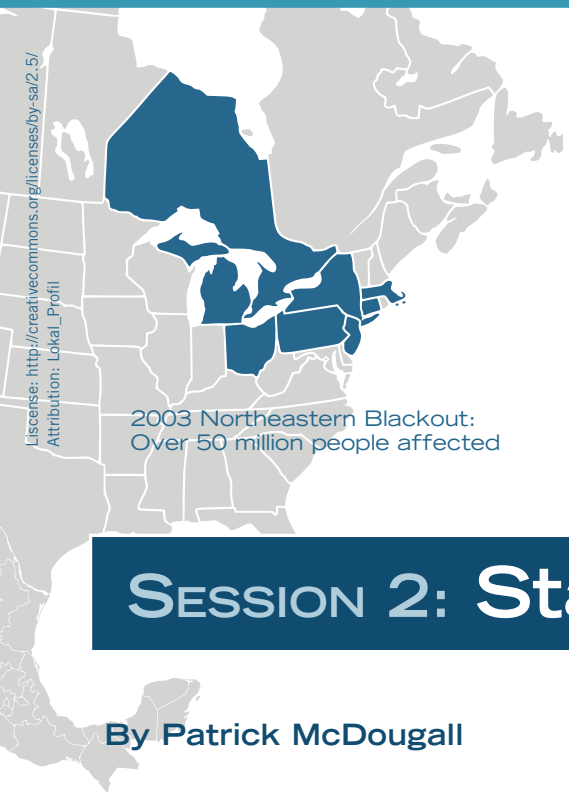
The Canadian Telecommunications Emergency Preparedness Association (CTEPA) is an exchange forum for major telecommunications companies. It includes Industry Canada's Emergency Telecommunications as a (non-voting) Associate Member and maintains access to international organizations such as NATO. CTEPA members, including Rogers and Aliant, exchange high-level, risk-related information to mitigate critical infrastructure threats despite a competitive environment where proprietary information is closely guarded.

CTEPA believes that securing Canada's telecommunications networks depends on a high level of trust among competitors and across the public and private sectors. The organization believes that successful collaboration requires a clear understanding of who needs what information, why it is important, and when sharing is necessary. CTEPA members exchange infrastructure protection information as well as share best practices and alternative opinions on threat reduction without disclosing specific risks. While CTEPA creates a safe forum for the exchange of sensitive information between private sector partners, telecommunications companies worry that sharing such information with others, including governments, creates a new vulnerability, potentially exposing proprietary information. Therefore, non disclosure and mutual aid agreements help to provide an appropriate context for collaboration.

Workshop participants debated the degree of caution in CIP-related risk management. Representatives from the private sector in particular, noted with concern government's propensity to be overly cautious, focusing on too many risks and perhaps failing to prioritize its efforts adequately, which ultimately drives up the cost of risk management.

Nevertheless, there was a consensus that government has an important role to play, particularly when it comes to coordinating responses to

> ...successful collaboration requires a clear understanding of **who needs what** information, why it is important, and when **sharing** is necessary.



2003 Northeastern Blackout:
Over 50 million people affected

multi-sectoral and multi-jurisdictional problems. The 2003 Northeastern Blackout served as an illustration. During this incident, Rogers' customers were without service because extreme demand for oil prevented the company from obtaining fuel for the backup generators that power its network. It was noted that governments can aid in preventing this type of failure by prioritizing which industries have guaranteed access to resources during crises. Ontario, for example, has over 400 municipalities with first-responder responsibilities. Absent some sort of government intervention, private companies would have to negotiate hundreds of individual fuel contracts in order to ensure necessary access to supplies during a shortage.

Session 2: Standards & Regulations

By Patrick McDougall

PRESENTER:

Bill Cove
Senior Analyst, Critical Infrastructure Policy Division, Public Safety Canada

Bill Cove presented Public Safety Canada's (PSC) *Working Towards a National Strategy and Action Plan for Critical Infrastructure (Plan)* which provides a common framework for federal and provincial/territorial governments and the private sector to increase the resilience of Canadian critical infrastructure. Recognizing the multi-organizational interdependence at work in protecting the nation's critical infrastructure, PSC views its role as providing national leadership by coordinating collaboration among the provinces/territories and the private sector.

The intent of PSC's *Plan* is to change behaviour through the engagement and voluntary compliance of stakeholders rather than by introducing new regulations. Specifically, the three objectives of the *Plan* are to build trusted and sustainable partnerships, implement an *all–hazards* approach to risk management and advance the timely sharing and protection of information among partners.

Cove's presentation sparked a dynamic discussion about the challenges of providing leadership for a pan-Canadian approach to CIP given the variety of partners involved from other levels of government and the private sector. Workshop participants discussed the merits of PSC's decision not to introduce new regulations, concerned that in their absence, major partners from industry

...the first step of the *Plan* should be to **build trust** and **regularize relationships**....

may simply not participate. Others agreed with the decision, believing that the first step of the *Plan* should be to build trust and regularize relationships in order to improve information-sharing among partners.

Participants discussed measurable outcome criteria for the *Plan*. One participant suggested PSC develop an evaluative framework and grade its partners according to a national CIP standard. Another participant suggested that PSC conduct a public opinion poll to see if Canadians feel safer following the *Plan's* implementation.

Participants noted the challenges posed by the cross-jurisdictional nature of CIP in Canada. Municipalities and local authorities are often the first responders in a crisis; however, these bodies are only indirectly represented by the provinces/territories in PSC's framework. One participant observed that Canada is increasingly becoming a country of large urban centres and suggested that cities should have a greater role than the provinces/territories which currently determine the extent of municipal involvement in PSC's *Plan*.

Another participant identified the need for a more dynamic system that can react to changing circumstances as the key to effective CIP and wondered whether PSC's *Plan* will encourage this or simply evolve into a checklist for compliance. While acknowledging this concern, other participants found that *Working Towards a National Strategy and Action Plan for Critical Infrastructure* facilitates dynamic planning, insofar as it provides leadership while ultimately allowing its partners to work together to develop their own CIP solutions.

For further discussion of PSC's *Plan*, please see interview with Daniel Lavoie on pages 4-5.

Session 3: Managing Behaviour Change

By Julie Davies

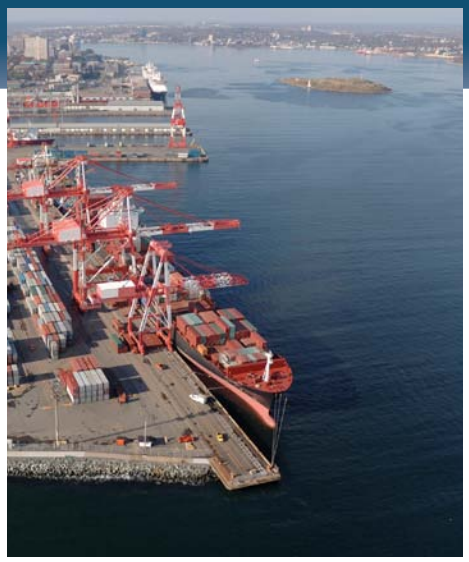
PRESENTERS:

Carl Yates
General Manager, Halifax Regional Water Commission (HRWC)

Charles Cirtwill
Executive Vice President, Atlantic Institute for Market Studies (AIMS)

Gudrun Curri
Associate Professor, School of Business Administration, Dalhousie University

Carl Yates opened his presentation by explaining the cultural shift that has occurred at the Halifax Regional Water Commission (HRWC) since 9/11. Prior to this event, the HRWC and other water utilities operated within a very open and transparent culture that included public tours of its facilities. However, in a post-9/11 world, there is a fine line between fostering open communication with the public and protecting information, even limiting site access in an industry now considered critical infrastructure. His biggest challenge in managing behaviour change has been convincing employees to make a culture shift towards one that takes safety and security more seriously. Yates noted with regret that there has been a slowness within the water utility industry generally to respond to security issues due to concerns surrounding negative publicity, exposure to future liability, financial restraints or simply the

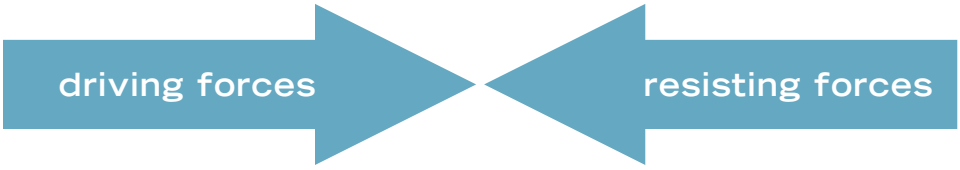


Halifax Harbour and Container Port

inability to discuss tactics in the absence of any security strategy. Ultimately, he feels that reporting security incidents must be mandatory rather than the current voluntary system.

Charles Cirtwill views measurement *and* reporting as the key to making change "matter." One of AIMS' biggest challenges lies in working with organizations to overcome the 'fear factor' and convincing them to move beyond their concerns about being blamed for poor results to using the data to implement change. A common obstacle in the public service is the idea that disclosure is an "all or nothing" exercise. In pointing out the difference between internal and external reporting, Cirtwill noted that the media only needs to know that you have an emergency plan; your employees need to know that you have a plan, what the plan is, and their role in it. Ultimately, appropriate disclosure is all about setting the context, which will then drive content.

Gudrun Curri discussed Lewin's Classic Change Model which involves three stages: *Un*freezing, where old attitudes, values and behaviours are weakened; Transforming, where training and skills development occur; and Refreezing, where new attitudes, values and behaviours mean that change has now become the *status quo*. She noted that it typically takes 7-10 years to change attitudes and that it is important to attain two-thirds of the change in the first third of your timeframe. Triggers for change can be either external or internal. External triggers can include changes in government regulations or technology, or even unexpected events like SARS or terrorist threats. Internal triggers can include restructuring or mergers and acquisitions. Curri warned that ignoring a trigger can result in 'boiled frog' syndrome in which we don't recognize the need for change until it's too late.



...the biggest challenge in managing **behaviour change** has been convincing employees to make a culture shift...

An animated discussion touched on how to convince companies to disclose information that they know will enter the public domain sooner or later. Ultimately, they face three choices: deny access, attack or engage with evaluators. Clearly, proactively managing the message is far more effective than trying to deny access or going on the defensive. Participants also explored the concept of the intrinsic value in 'resiliency,' where someone could buy a company with minimal resiliency, make it more resilient (for example, by adopting emergency plans etc.,) and sell it at a higher value. A company in the U.S., for instance, has created an index that measures organizational resiliency. It uses the index to grade various companies publicly. Through the use of public disclosure, the company hopes to pressure those companies with weak records into changing their ways. Other questions at the session involved vulnerability brought about by interdependence—for instance, if a company's supplier has poor contingency plans, should the company *buy* the supplier and thereby reduce the company's risk exposure? Or would government be better placed to regulate these types of problems?

Ultimately, they face **three** choices: deny access, attack or engage with evaluators.

Session 4: Legal Challenges & Market Constraints

By Patrick McDougall

PRESENTERS:

Brian Booth
Director, Technology and C4ISR Business Development, General Dynamics

Jez Littlewood
Director, Canadian Centre of Intelligence and Security Studies, Carleton University

General Dynamics' Brian Booth explained that markets do not always lend themselves to the cooperative dynamic that we might like to see in pan-economic CIP. He noted, for instance, private companies are hesitant to share information about their vulnerabilities to avoid competitors exploiting any perceived weaknesses. Governments are often limited in their ability to assist since they do not always have the knowledge to regulate every market given the speed of technological change in certain industries. Booth concluded that self-regulation on the part of industry through professional groups and associations offers perhaps the greatest potential.

He did see an opportunity for an expanded role for government, however. Given the interdependency of critical infrastructure, Booth noted a plan is necessary to establish cooperation across governmental jurisdictions and the private sector, and government is uniquely positioned to carry out this task. However, margins are tight; therefore any kind of national CIP plan, such as Public Safety Canada's *Working Towards a National Strategy and Action Plan for Critical Infrastructure,* needs to provide funding for industry to participate.

Appropriate disclosure and legal liability were central themes of Jez Littlewood's presentation of Jacques Shore's paper, "The Legal Imperative to Protect Critical Energy Infrastructure."[1] For instance, Littlewood explained that ministers are responsible for identifying their own department's vulnerabilities and failure to develop adequate plans to respond to those vulnerabilities may result in legal liability. Crucially, to ensure preparedness, departments must also secure cooperation with their private sector critical infrastructure partners.

Littlewood noted that the issue of government liability has already arisen in the U.S. where the Port Authority of New York and New Jersey was successfully sued for negligent security practices following the 1993 bombing of the World Trade Center. Similar actions were brought against the Ontario government following its handling of the 2003 SARS outbreak. Although the SARS cases were ultimately dismissed, Littlewood believes that legal liability will become an increasingly important issue. Workshop participants from industry agreed, adding that legal liability is already affecting many decisions to the point where their companies have walked away from contracts with liability issues.

Littlewood presents Shore's paper on legal issues

Participants expanded on Booth's initial assessment that the optimal level of CIP comes down to a question of acceptable costs, whether they are financial costs or limitations to personal freedom. Workshop participants agreed that the costs of CIP are ultimately transferred to the general public in their capacity as consumers, taxpayers and citizens.

> ...legal liability is already affecting many decisions ...companies have walked away from contracts...

[1] Shore, Jacques, "The Legal Imperative to Protect Critical Energy Infrastructure." Critical Energy Infrastructure Protection Policy Research Series, March 2008, No. 2. The Canadian Centre of Intelligence and Security Studies (CCISS) at Carleton University. Available on-line at http://www.carleton.ca/cciss/ceipprs_publications/shore_02_2008.pdf.

Session 5: Technical Issues

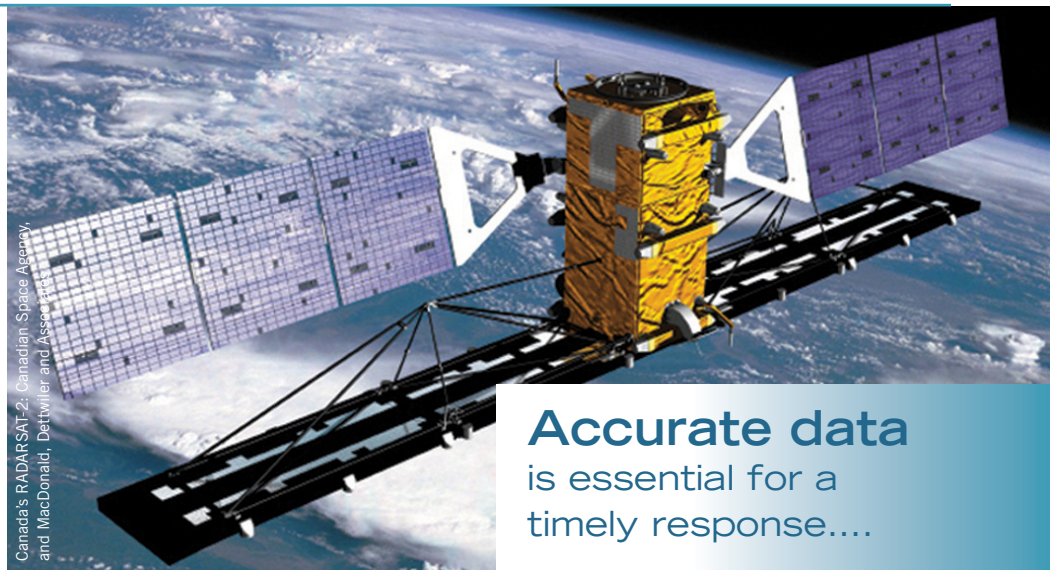
By Craig O'Blenis

PRESENTERS:

Paul Adlakha
Director, Marketing, C-CORE

Jeff Fraser
Manager, Medical Communications Centre & System Status Planning, Nova Scotia's Emergency Health Services

Paul Gareau
IT Systems Consultant, Ambulance Operations Management, Nova Scotia's Emergency Health Services



Canada's RADARSAT-2: Canadian Space Agency, and MacDonald, Dettwiler and Associates

Accurate data is essential for a timely response....

Technology has become an essential feature of safety- and security-related products and services in many sectors. This session discussed how service providers and end-users can use technology to prevent *and* respond to circumstances that might otherwise damage critical infrastructure.

From the perspective of prevention, C-CORE's satellite and radar monitoring services help companies identify intrusions and monitor asset integrity. C-CORE is in the process of developing high-powered satellites capable of capturing detailed information on environmental or structural changes surrounding company assets. Combined with faster satellites, C-CORE believes that this technology has cross-sectoral applications for critical infrastructure protection, including pipeline building, real estate development and port security. There are concerns, however. Most governments, for instance, have security regulations prohibiting the use of many types of images that satellites produce. Relatedly, and as noted in the discussion, jurisdictional confusion prevents companies from maximizing the use of available satellite data. There are also technical complexities that prevent the technology from being used to its full potential, such as the challenge of correlating data collected through different frequencies and even moisture's impact on radar signals. On the response side, Nova Scotia Emergency Health Services (EHS) relies on seamless technology integration for rapid responses in emergency situations. With four contact centres in the province, EHS integrates GPS with both wired and wireless communications to ensure that each centre knows the exact location of ambulances, ambulance response times, and caller information. Accurate data is essential for a timely response and if information in one record does not correlate with data in another, critical response time suffers. As a user, EHS is at the mercy of hardware and software vendors; therefore, it exercises a somewhat conservative approach in waiting for other agencies to implement new technologies first, which allows EHS to avoid many of the problems common in system upgrades.

Discussion focused on the perceived gap between those people *creating* risk management strategies and those *implementing* risk management strategies. Many noted that managers' experiences of risk and risk management may not coincide with front-line realities. At the same time, front-line operators are not always kept up-to-date on the most recent organizational plans.

Session 6:
Institutions & Jurisdictions

By Julie Davies

PRESENTERS:

Keith McGuire
Emergency Management/Operational Readiness and Response Coordination Centre, RCMP

Russell Stuart
Director, Nova Scotia Health Services Emergency Management

Opening his presentation by quoting directly from relevant legislation,[1] Keith McGuire refers to the importance of legal context within jurisdictional responsibilities. In terms of terrorism, the RCMP has the primary role in investigation and apprehension with a mandate that crosses most borders and jurisdictions in Canada. Several key assumptions exist: no one organization, either public, private or non-governmental, has the resources and expertise to respond unilaterally to terrorism; roles and responsibilities among these groups will likely overlap; first responders will have to manage any incident while working with existing local resources and expertise until outside provincial/territorial/federal agencies arrive; and a major act of terrorism may overwhelm local, provincial and even federal resources and expertise. Therefore, a legal framework clarifies critical roles and responsibilities in complex environments typical of serious terrorist attacks; at the same time a degree of flexibility among critical stakeholders is likely required.

Understanding who holds responsibility for taking the lead in emergency response is critical. During the SARS crisis in Toronto, it took two weeks for a decision to be made on who had the leadership role in this event, noted Russell Stuart of Nova Scotia Health Services Emergency Management. He also noted that creating 'a common lexicon' facilitates CIP discussions across jurisdictions and cultures to facilitate information-sharing using tools such as a *Hazard Vulnerability Table*. This table uses a colour-coded system to distinguish between threats (in terms of probability) and between degrees of impact or consequences. However, limitations exist, as Stuart acknowledges. For instance, the *Table* helps in setting priorities, but it doesn't tell you how to respond. Indeed, one of the challenges in CIP is striking a balance between an inadequate response and overreaction.

> ...no one organization... has the resources and expertise to respond unilaterally to terrorism....

McGuire discusses the role of the RCMP in emergency response

Much of the discussion focused on communications and strategic messaging during crisis situations. One participant noted that, depending on the nature of the event, politicians and political staff might play a larger role in the emergency response. This can create a new dynamic with which operational staff must contend, given that political staff are not always involved in routine emergency preparedness exercises. One participant questioned the role of politicians in communications and the media, in particular. Ultimately, Stuart feels that under the appropriate circumstances the role of politicians is to reassure citizens, citing Tony Blair standing in a subway station shortly after the 7/7 terrorist bombs as an example.

[1] *Security Offences Act*, R.S.C. 1985, c. S-7, s2, s6(1).

VIRTUALLY POSSIBLE:

New approaches to distance education and collaboration

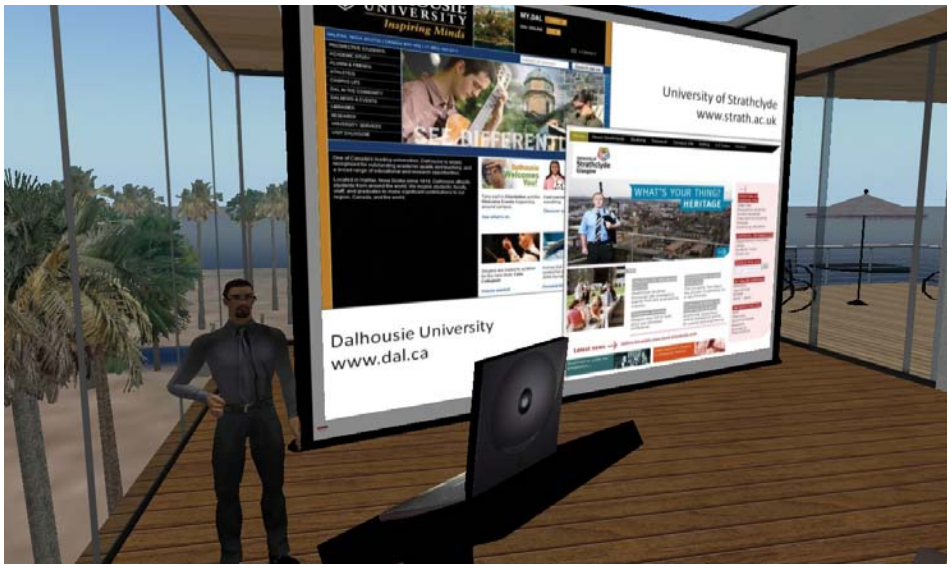
By Howard Ramsay

As part of the Critical Infrastructure Protection Initiative, on November 18th Dalhousie University and the University of Strathclyde in Glasgow, Scotland will run a live transatlantic seminar in the virtual world *Second Life* (www.secondlife.com). Peter Bennett, Head of Operational Research for the Department of Health in London, will discuss risk communication in the health field. *(See following page for details on Bennett's talk.)*

Second Life is emerging as an exciting new vehicle for distance education and collaboration. Companies such as IBM and Cisco have set up their own branded and customized areas in this innovative online world for training and research purposes.

In *Second Life* participants appear as "avatars" – graphical representations that walk around the environment and communicate in real time with other participants.

Second Life seminar space brings people together with relative ease and provides the tools for extensive collaboration. Supporting audio, video and presentation facilities, the seminar facilities allow up to 160 participants to connect from anywhere in the world. While video conferencing can provide speaker-to-participant contact, *Second Life* is noted for enabling greater communication between participants. In fact, early research suggests that when using *Second Life*, audiences arrive earlier and leave later than with conventional video conferences.



Howard Ramsay's avatar in the University of Strathclyde's virtual seminar room

Overhead and carbon footprints are dramatically reduced. The only requirements are a broadband connection, a relatively new PC/Macintosh and a headset with microphone.

Overhead and carbon footprints are dramatically reduced.

There are some challenges. It is relatively new software. The technical requirements can hinder participation and experience has shown that first-time participants need an induction session to get on top of the mechanics of the virtual world. Like many software tools, however, users seem to be more comfortable with it the more often they use it.

If you would like to participate in our test of *Second Life* on November 18th, please see the ad on the next page for further details.

Howard Ramsay is an educational technologist at the University of Strathclyde Business School. For more information on the research on *Second Life* at Strathclyde University, please contact Howard at howard.ramsay@strath.ac.uk

Health communication seminar in virtual world *Second Life* on November 18th

SEMINAR: Communicating about risks to public health

Peter Bennett
November 18th, 11:30-1 pm, Atlantic (10:30-12 EST)

This seminar considers some of the most important factors affecting communication about risks to public health – i.e. real or alleged hazards that might affect many people within the population.

Public reactions to risk sometimes seem bizarre, at least when compared with scientific estimates. Though risk may technically be defined as "probability times severity of harm," the suggestion that a hazard poses an annual risk of death of "one chance in x" may cause near-panic or virtual indifference. But such reactions are not totally unpredictable - or even necessarily unreasonable. Over the last thirty years, there has been a progressive change in the literature on risk communication:

- from an original emphasis on "public misperceptions of risk," which tended to treat all deviations from expert estimates as products of ignorance or stupidity,
- via investigation of what actually does cause concern and why,
- to approaches which promote risk communication as a two-way process in which both "expert" and "lay" perspectives should inform each other.

This is not to deny that misperceptions exist: people may sometimes be most fearful of the "wrong" hazards. Even if the aim is to change such views, however, one needs to understand how they arise. More fundamentally, misperceptions do not affect only "the public." There is good evidence to suggest that everyone - public and "expert" alike - is fallible when thinking about risk. At the same time, debates on risk need to be seen within a wider social and political context, in which fundamental values may be in dispute.

The talk will discuss some key findings from research on risk perception and communication, and their implications for practice.

Dr. Peter Bennett

Following a first degree in Physics and a doctorate in Philosophy of Science, Peter joined the Operational Research Group at Sussex University, and then moved to Strathclyde University, becoming Reader in Management Science and Director of Postgraduate Studies. He joined the Department of Health as a Principal OR Analyst in 1996, and since then has been heavily involved in analyses of risks to public health. He produced the Department of Health guidelines on risk communication, and the volume *Risk Communication and Public Health*, co-edited by Sir Kenneth Calman and published by Oxford University Press (a new edition of which will appear in 2009). He has led the production of risk assessments in several different areas, but particularly on the risks of variant CJD being spread by blood transfusion or re-use of surgical instruments. These are areas in which scientific uncertainty magnifies the challenges of effective risk communication. He now leads a cross-disciplinary team of analysts in the Heath Protection Directorate of Department of Health, and is Head of Operational Research for DH in London.

Two ways to attend the seminar:

On campus: 6100 University Ave, Rowe Building, Room 1016, Dalhousie University to watch the seminar on the big screen. There is no charge to attend. Seating is limited, first come, first served.

Remotely: If you wish to log onto the event yourself please contact Howard Ramsay (howard.ramsay@strath.ac.uk) at your earliest convenience.

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: