THE CIP EXCHANGE

A forum for sharing views and information about critical infrastructure protection SPRING 2009

Seven Questions for Michael Chertoff

Former head of US Homeland Security discusses the flu, government/industry interactions, cyber and border security

DALHOUSIE UNIVERSITY Inspiring Minds Faculty of Management School of Public Administration

CONTENTS

EDITORIAL

Editor: Kevin Quigley

Assistant Editor: Julia McCarthy

Copy Editor: Janet Lord

Design: Dalhousie Design Services, Roxanna Boers, Designer

Additional Thanks: Ron Pelot, Industrial Engineering at Dalhousie

On February 15, 2005, the United States Congress unanimously approved President Bush's nomination for Secretary of Homeland Security, Michael Chertoff. As Secretary, he reported directly to President Bush on a wide range of domestic and international security issues. Prior to accepting the offer to serve in this capacity, Mr. Chertoff was a judge in the US Court of Appeals. He had also held several prominent positions in President Bush's administration, including Assistant Attorney General in the Criminal Division of the Justice Department. While at the Justice Department, Mr. Chertoff took a lead role in drafting the *USA PATRIOT Act*. The early part of Mr. Chertoff's career is notable for his work in the prosecution of high profile mafia and political corruption cases. He now works at the law firm Covington & Burling and has recently started his own risk management firm to advise corporate clients and governments on security issues. Kevin Quigley interviewed Michael Chertoff by telephone on May 6, 2009.

Michael Chertoff

KQ: What do you think the most challenging aspect of responding to the current outbreak of swine flu will be for the new Secretary of Homeland Security? How would you advise her to overcome that challenge?

MC: The challenge is to make sure that people become focused on the preparations they need to conduct as businesses and individuals so that if in fact it becomes a more serious form of flu they will be ready. The only way to meet the challenge is to continue to relentlessly remind people of the importance of preparation.

KQ: Government critical infrastructure protection plans frequently refer to the importance of developing 'trusted relationships' (e.g., between government agencies; between

public sector and private sector). Yet the complexity of modern critical infrastructure makes information at times unreliable. Information in this area can also be classified or deliberately withheld for competitive reasons. Does this uncertainty undermine our capacity to develop trusted relationships with respect to critical infrastructure protection? What can we do to strengthen our capacity to develop trusted relationships?

MC: The best way to handle the situation is to create an ability to declassify information or lower the classification of material. We also have to assure businesses that when they convey market-sensitive information to government it will be held confidentially and will not be subject to freedom of information requests. This strategy has worked reasonably well for us.

> "We did not try to eliminate the risk, but we would think about the measures that were cost-effective in reducing the risk."

KQ: In the past you have noted that trade-offs are necessary in any risk management plan. When confronted with difficult trade-offs as Secretary, what guided your reasoning in the positions you took or the balance you sought to achieve?

MC: The main principles were to accurately identify the risk—that is, the threat, the vulnerability and the consequence. We did not try to eliminate the risk, but we would think about the measures that were cost-effective in reducing the risk. We avoided imposing measures that did not relate to the outcome.

KQ: How did you engage the various stakeholders on this question?

MC: Often what we would do is put up performance standards for businesses but allow them to tailor the way they achieved the results.

KQ: You have said in the past that cybersecurity is your greatest (short-term) concern. What needs to be done to allay your concerns?

MC: I think the government needs to continue to build on the cybersecurity strategy that we put together last year, which means adequately funding and building out the institutional capability to protect the network. The government also needs to create legal and other incentives for the private sector to quality-assure the hardware and software they acquire and make sure the internal security of their systems is being properly maintained.

KQ: Where is the need for greater collaboration between the US and Canada the most urgent? What constrains this collaboration? What potential exists to improve it?

MC: There are some differences in the legal systems. The authority that Canadian officials have with respect to people coming into Canada is different from the authority American officials have when people try to enter the US. This asymmetry tends to create a greater demand on the American side. We put measures in place to double-check people coming in from Canada. The more you can synchronize these authorities the easier it will be to move between the countries, but I don't think there will ever be a perfect synchronization.

KQ: With respect to legal differences, were there particular issues that had to be managed?

MC: Canadian officials have less authority than American officials to ask questions of, search or obtain biometrics from people entering the country. That means it is easier to get into the North American continent through Canada than it is through the United States, and that's asymmetry.

For a copy of the Department of Homeland Security's Strategic Plan, please visit the DHS website: http://www.dhs.gov/xabout/strategicplan/

Guiding Principles of DHS's Strategic Plan (2008-2013):

- Protect Constitutional Rights and American Values
- Use an *All-Hazards* Approach
- Build Trust through Collaboration and Partnerships
- Apply Risk Management
- Develop a Culture of Preparedness
- Ensure Accountability
- Capitalize on Emerging Technologies
- Work as an Integrated Response Team
- Be Flexible

London Calling

Second Life software connects Halifax with Glasgow and London for Risk and Public Health Seminar

by Elisa Obermann

Risk communication has become an integral part of risk management strategies that seek to address public health and safety issues. Probabilities and risk comparisons are often used to illustrate the severity or (un)likelihood of a particular event occurring, but these methods, if poorly communicated, can trigger unanticipated and undesirable public reactions.

On November 18, 2008, Dr. Peter Bennett, Head of Operational Research for the Department of Health in London and co-editor of *Risk Communication and Public Health*,[1] elaborated on the importance of risk communication in public health. The seminar was held by Dalhousie University in Halifax and the University of Strathclyde in Glasgow, as part of the Critical Infrastructure Protection Initiative. With Bennett located in London, the seminar was broadcast to audiences in Canada, England and Scotland through the use of the virtual world software *Second Life*. The audience at Dalhousie was able to view Bennett's *Second Life* "avatar" and slide presentation in real time on a projection screen while participating in the discussion and posing questions through the software.

Estimating risks and communicating about them is not just about using conventional methods such as 'probability x consequence,' Bennett noted. Although this traditional quantitative approach often underpins the rationale for risk communication, the approach can be limited in its ability to take important emotional and cognitive factors into consideration. According to Bennett, communication strategists must consider whether the intended audience knows and understands the risk in question; they must also consider the level of anxiety people feel about

The University of Strathclyde's *Second Life* seminar room

> ...strategists must consider whether the **intended audience** knows and understands the risk in question...

[1] Bennett, P. (1999). *Risk Communication and Public Health.* New York: Oxford University Press.

Photos: Nick Pearce

Practitioners, faculty and students attended the event in person or logged in from remote locations

...they must also consider the **level of anxiety** people feel about the risk.

the risk. Messages about road safety and cancer threats prompt different emotional responses, for instance. Without this awareness, generalized risk communication plans can often fail to include important nuances that can help to achieve the desired effect on the intended audience.

Risk perception can also be skewed by individual biases and framing techniques. Events that are dramatic and memorable are thought to be more probable and dangerous than mundane, everyday activities, he noted, even when the probability and consequence data might suggest otherwise.

Throughout the seminar, Bennett emphasized the role of values. People will weigh the riskiness of a situation according to their beliefs. While it is clear that people have different values, it is not as straightforward to determine how these values specifically affect risk perception and behaviour. Bennett cited Cultural Theory as a possible aid. Cultural Theory categorizes people into one of four groups—individualist, egalitarian, hierarchist and fatalist. Each group represents an extreme set of values and way of thinking about risk. While hierarchists believe appropriate expertise and bureaucratic structures are the best means to mitigate risk, individualists see risk as something to be desired, or as an opportunity to exploit. If individuals or organizations are categorized under one of these groups, it may be easier to understand how they will respond to particular risks.

Since identifying some of these challenges surrounding risk in the late 1990's, the Department of Health in London has been working towards improved risk communication. Bennett noted that their policy process has devised several tools to increase the effectiveness of the Department's practice. He suggested governments should be encouraged to think about how stakeholders should be classified, to analyze uncertainties more broadly, and to consider the robustness of future risk communication strategies in light of some of the observations he noted.

Elisa Obermann is a recent graduate of Dalhousie University's Master of Public Administration Program.

People will weigh the riskiness of a situation according to **their beliefs**.

Many Questions, Some Answers at Carleton/ Public Safety Canada Workshop:

Academics and Practitioners Exchange Views on 'Resilience'

by Jez Littlewood

On December 15, 2008, the Canadian Centre of Intelligence and Security Studies (CCISS) at Carleton University (Ottawa) hosted a workshop on "Resilience in Canada" in cooperation with Public Safety Canada under the latter's policy development contribution program. The day-long workshop brought together individuals from academia and government departments and associations to consider the issue of "resilience." (See box on next page for list of participating organizations.)

Discussions were organized around three broad themes: (1) infrastructure protection and resilience; (2) individual and population health; and (3) community characteristics. A working lunch allowed Keith Weston (Cranfield, UK) and Steve Recca (Colorado Springs, USA) to report on UK, US and Australian perspectives on the issue of resilience. The final session aimed to bridge the gap between the themes and identify issues that required further consideration.

A number of issues were identified by participants across panels and in the discussions that followed. First, the sheer complexity of the challenges faced by all parties—federal, provincial and municipal governments, businesses, public sector organizations, communities and individuals—can be daunting. Any disaster or major disrupting event presents discrete challenges that require detailed contextual knowledge and awareness. At the same time, limited resources constrain what governments and local communities can do to prepare. As such, stakeholders have tended towards an *all-hazards* approach, which is vulnerable to neglecting important nuances. This underscored the requirement for a number of actions that are in one sense insurance activities that will prove their worth only in the face of an actual event. These actions included, for instance, liaising with as many partners as possible, training, scenario-planning and testing preparatory systems. More generally, stakeholders should try to identify weaknesses in planned

Any disaster or major disrupting event presents discrete challenges that require detailed contextual knowledge and awareness.

Carleton University in Ottawa, Canada

...in terms of **resilience**, economic factors... political factors... and environmental and psychological issues **all** have to be included in assessment and preparatory efforts.

responses as well as uncover unanticipated or unforeseen problems.

A second theme was the different perspectives on what resilience actually is and how it might be explored. Several interpretations of the term were put in play: social- and community-based definitions; the term as it relates to the engineering of physical structures; and the social ecology and natural environment understanding. These discussions prompted observations about interdependencies between physical and natural systems and governance structures. It also raised important questions about short- and long-term perspectives in emergency response and notions of resilience. For example, an event may elicit effects that have physical, economic, political, environmental and psychological dimensions. Physical impacts (e.g., deaths, injuries, damage to infrastructure) often form the basis of assessments in the short term. Yet in terms of resilience, economic factors (e.g., business continuity, minimizing detrimental economic effects), political factors (e.g., trust in decision makers and governance structures, whether or not emergency plans actually work satisfactorily) and environmental and psychological issues all have to be included in assessment and preparatory efforts. Examinations of the SARS outbreak (2003), the handling of Hurricane Katrina in the United States (2005) or the Foot and Mouth disease outbreak in the UK (2001), for instance, reveal the myriad factors that impact our capacity to recover.

...different communities and **perspectives** served to underline that resilience is an amorphous concept.

A third theme was how to measure resilience and changes in it. The notion that one cannot manage without appropriate metrics raised both philosophical and pragmatic responses. One approach was to attempt to measure what governments should do, as well as what governments could do, such as planning, exercises and training, awareness-raising and information-exchange. A complementary approach considered the different types of metrics that might be used to assess the level of resilience along a spectrum. Appraisals of the state of play both "before" and "after" efforts to increase resilience were seen as necessary baselines. This led participants into a discussion on appropriate information-sharing and levels of transparency. It also led them to consider what motivates individuals, businesses and other sectors to change behaviour: education and awareness of hazards and threats, economic factors relating to business continuity, or emotional responses to either of these?

The workshop did not produce answers to any of the above issues; rather, the different communities and perspectives served to underline that resilience is an amorphous concept. Understanding those different approaches and the contexts in which resilience planning has to occur does not provide a solution to any problems by itself; rather, such understanding can contribute to both local (tactical) and national (strategic) policy development.

Jez Littlewood is the Director of the Canadian Centre of Intelligence and Security Studies at the Norman Paterson School of International Affairs, Carleton University, Ottawa.

Participating Organizations

Brandon University
Carleton University
Cranfield University (UK)
Dalhousie University
Defence Research and Development Canada
- Centre for Security Science
Federation of Canadian Municipalities
Public Safety Canada
- National Crime Prevention Centre
- Aboriginal Policing Directorate
Royal Canadian Mounted Police
University of Ottawa
University of Waterloo
University of Colorado at Colorado Springs (USA)
York University

Reflections on RUSI's Critical National Infrastructure (CNI) 2009 Conference:
Protecting Critical Infrastructure in a Changing World

by Tobias Feakin

Editor's Note: The Royal United Services Institute (RUSI), founded in 1831, is an independent institution that fosters free discussion and careful reflection on matters of security and defence. RUSI is located in Whitehall, London, England. It has satellite offices in Doha, Qatar, and Washington, DC.

RUSI's approach to examining CNI is very much consistent with the conceptual thrust behind the UK's *National Security Strategy*[1] which says we should first think about the essence of what it is in our society that we want to protect and defend, and then move outward. In this way RUSI looks at CNI in its broadest sense, be it conceptually/theoretically, questions of policy, examining vulnerabilities, energy issues or climate change and the international dimensions of those issues. The CNI Conference at RUSI encapsulated this thinking over the course of two days on April 29 and 30.

> Our use of information and communication technology…facilitates new dependencies and thus vulnerabilities.

The world is going through a period of change more rapid and arguably more significant than at any other time in its modern history. The degree and speed of change impact profoundly the critical infrastructures on which states rely. The complexities of a globalized economy and society mean that a power outage in the Netherlands could very quickly become a power outage across most of Western Europe. This complexity means that there are new vulnerabilities we need to consider and understand. Climate change will entail huge upheavals in the long term, but already it is linked to increasingly frequent bouts of extreme weather. Our use of information and communication technology continues to break new ground, but also facilitates new dependencies and thus vulnerabilities. The networks, which our most vital infrastructure is part of, and dependent upon, have become so complex that they are almost impossible to analyze fully. Our systems are more tightly coupled and susceptible to cascading failures, while our society and economy are less resilient than ever to temporary disruptions. There is also a psychological dimension to this issue. One of the consequences of the present financial crisis is that we are in some ways reassessing the relationship between the citizen and the state in terms of what the state should and should not do in the economy. Indeed, protecting CNI is as much about our collective psychology as it is the physical facilities that the state provides.

A number of interesting themes emerged from the conference. Lord West, the Government's Security and Counter Terrorism Minister, made it clear that the threat to critical infrastructure from terrorism continues to occupy much of the government's thinking on the subject. Aside from these malicious threats, the Civil Contingencies Secretariat (CCS) offered more detail on a new program of work that it is undertaking in response to the Pitt Review of the summer flooding in 2007.[2] The failures

[1] UK Cabinet Office (2008), *The National Security Strategy of the United Kingdom: Security in an Interdependent World.* Available online: http://interactive.cabinetoffice.gov.uk/documents/security/national_security_strategy.pdf
[2] For more information on the Pitt Review, please see http://archive.cabinetoffice.gov.uk/pittreview/thepittreview.html

> ...regulators have indulged in the **'sweating'** of assets as they have competed to drive down prices for consumers at the expense of building up long-term capacity in the system.

of critical infrastructure caused by the flooding were much more costly than the direct flood damage, and their consequences for local people and businesses lasted much longer. The entire episode exposed important weaknesses in the way that government advises owners and operators of critical infrastructure on non-malicious threats. CCS seeks to address these issues.

Senior speakers from the US Department of Homeland Security and the European Union (EU) were able to offer some insight into the way that new infrastructure challenges were being met elsewhere. Being increasingly confident about the level of protection it is able to afford internal infrastructure, the US is now turning its attention to dependencies that originate outside its borders. Similarly, the increasingly interdependent nature of the EU has been driving more ambitious initiatives from the European Commission. Conference delegates were updated on a number of initiatives, such as the European Programme for Critical Infrastructure Protection (EPCIP),[3] that aim to address pan-European infrastructure vulnerabilities in a more coherent fashion.

The number of international speakers and guests at the conference gave ample opportunity for comparisons of national critical infrastructure regimes around the world. The UK is certainly well thought of, if not envied by many of its international partners in terms of its preparations for external shocks and the work it has done on countering terrorist threats. However, what became clear through the conference was that there were a number of systemic governance issues which will have to be addressed if the UK is to meet the challenges of a changing world. Among these, the question of regulation appears to be the most pressing.

For those who were not already aware, what emerged starkly from the conference was the fact that the system of regulation and regulators that currently surrounds our essential services is severely lacking and is undermining our efforts to achieve a secure and resilient national infrastructure. The UK currently works under a regulatory regime that is designed for utilities as they were, not as they are. Oxford University's Dieter Helm, in particular, painted a vivid picture of regulators operating in silos, focussing on the essential service for which they are responsible with no regard for the complexities and interdependencies that are now a feature of our essential services. Further, price setting by the regulators takes almost no account of the need to build in or maintain redundancy. Historically, regulators have indulged in the 'sweating' of assets as they have competed to drive down prices for consumers at the expense of building up long-term capacity in the system. If this were to continue, it would leave the UK in a perilous state; reform of the regulatory system, many concluded, must now be a priority.

Dr. Tobias Feakin is Director, National Security and Resilience, at RUSI. For more information about RUSI's CNI research program please contact Dr. Feakin, tobiasf@rusi.org

Presentations from *CNI 2009: Protecting Critical Infrastructure in a Changing World* are available for download at www.rusi.org/CNI2009

[3] For more information on this program please see http://ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm

ADVANCING the Profession

SARMA Hosts Upcoming Conference in Arlington, Virginia, on Risk and Security Analysis

by Ed Jopeck

In the US, risk analysis and risk management remain areas of intense interest for the homeland security community. The Security Analysis and Risk Management Association (SARMA), the leading non-profit professional association in the field, provides an open and independent venue for federal, state and local governments to engage with security professionals and experts at all levels.

SARMA's third annual conference, *New Perspectives on Security Risk Management*, will be held June 16-18 in Arlington, Virginia. The conference will feature presentations from the top leaders in the homeland security, defense and intelligence communities. Seasoned security professionals and academic specialists will share their perspectives and discuss their successes —all in the name of advancing the profession of security risk analysis.

In addition, luminaries from the US and abroad will be in attendance at a SARMA social event on the eve of the conference. One such luminary is the former Secretary of Homeland Security, the Honorable Michael Chertoff, who will receive special recognition at the event from SARMA for his contributions to developing the field of security risk management in homeland security.

Among the many speakers confirmed to speak at the conference thus far are the directors of the US Department of

2009 SARMA Conference June 16-18

Larry J. Clark

SARMA's 2008 conference

Homeland Security's Office of Risk Management and Analysis, its Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and its Office of Infrastructure Protection. There will also be an expanded international component this year. Representing Dalhousie University will be Kevin Quigley, who will speak on Public Safety Canada's *Draft National Strategy and Action Plan for Critical Infrastructure*. "It's an ideal opportunity for practitioners and academics to exchange views on the important safety and security issues that many countries are dealing with," Quigley said.

"This year's conference is unique in the level of international participation expected," said SARMA's President, Kerry Thomas. "As the profession grows, the barriers to progress created by geographical and organizational boundaries are becoming less and less relevant. This profession is healthy and expanding rapidly," he concluded.

For more information on SARMA and the third annual conference visit www.sarma.org

Ed Jopeck is the Immediate Past President of SARMA.

Larry J. Clark

Ed Jopeck

LEVERAGING TECHNOLOGIES

CARVER + Shock

An Operational Risk Management Tool for the Agri-Food Sector

by Andrew J. Tidball

Last year's listeriosis outbreak in Canada was a stark reminder that the infrastructure that underpins food supply is indeed crucial to the well-being of the country and subject to failures with serious consequences. What is perhaps most striking about the aftermath of the outbreak is the very public commitment that the president of Maple Leaf Foods, Michael McCain, has made to reducing the likelihood of such an event recurring. Maple Leaf Foods' size and resources make it an anomaly in the food sector, however. Many food suppliers are in fact small and medium-sized enterprises (SMEs) and have fewer resources to dedicate to risk management practices. This is a challenge for the sector and for those concerned with the safety of the food supply generally.

In the US, policymakers have tried to meet this challenge by developing on-line risk management tools, which include process mapping and risk self assessments for SMEs. CARVER + Shock is one such example. The Food and Drug Administration's (FDA) Center for Food Safety and Applied Nutrition modified the tool from its original military purpose to help users evaluate security and terrorism-related risks in their organizations.[1] The tool examines seven aspects of potential targets: criticality, accessibility, recoverability, vulnerability, effect and recognizability (CARVER). 'Shock' is a seventh attribute, the FDA's website notes, added to

[1] CARVER + Shock is designed to be implemented in conjunction with the Food and Agriculture System Criticality Assessment Tool (FAS-CAT) developed by the National Center for Food Protection and Defence at the Department of Homeland Security. It can be downloaded from the FoodSHIELD website: http://www.foodshield.org/criticality/.

The development of independent software programs to help SMEs is a step in the right direction.

"assess the combined health, economic and psychological impacts of an attack within the food industry."

The tool is available as a free download from the FDA website.[2] Industry participants are asked a series of questions pertaining to their production facilities, and are then provided with a risk score from 1 to 10 in each of the seven attribute areas. The score indicates the "target attractiveness" for each stage (or node) of the production process. CARVER + Shock allows SMEs to self-evaluate with a level of anonymity and in a cost-effective manner. It also encourages participants to at least consider certain FDA standards and best practices. The benefits may not accrue strictly to the participants, however. It would seem that the standardized scoring system can permit policy makers to aggregate data in order to gain insights into the sector as a whole.

Tools such as these have inevitable constraints. The voluntary nature of CARVER + Shock, for instance, will limit the numbers who choose to participate. It's also not clear whether SMEs will actually act on the information they learn through the tools. The fact that the FDA cannot monitor the use and impact of this tool limits the FDA's ability to evaluate the tool's overall effectiveness.

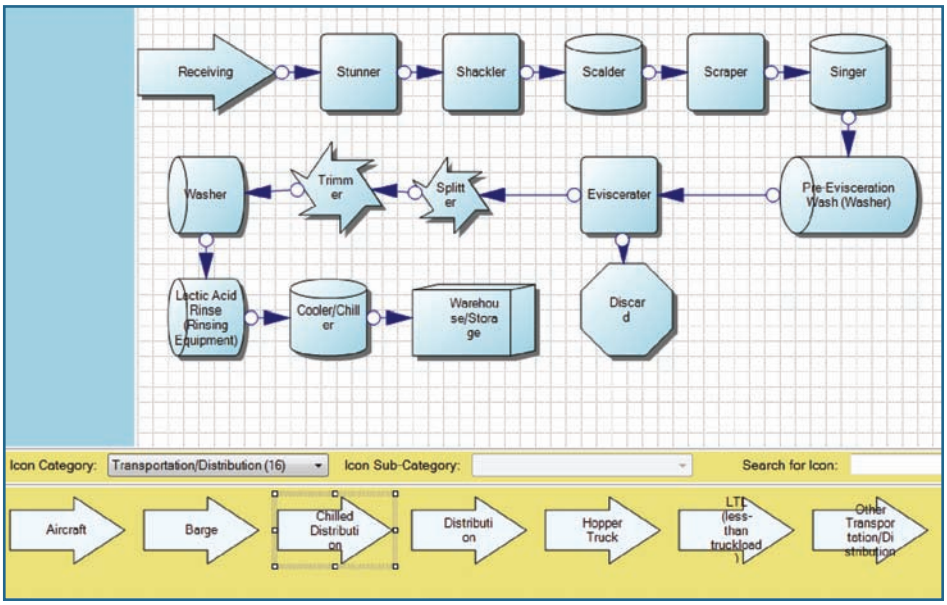


Figure 1: A standard template of the production process of an animal slaughterhouse, modelled in the CARVER + Shock program. Each blue symbol within the grid represents a stage (or node) in the production process. Participants can add stages (depicted in the yellow band at bottom) to tailor the model to individual SMEs.

Nevertheless, CARVER + Shock is a notable advance in CIP in the agri-food sector. The development of independent software programs to help SMEs is a step in the right direction. The question now is whether tools such as these can be used more flexibly, beyond the food sector, for instance, or for risks other than that of terrorism.

Andrew Tidball is a recent graduate of Dalhousie University's Master of Public Administration Program.

[2] CARVER + Shock Download: http://www.fda.gov/Food/FoodDefense/CARVER/default.htm

Ambitious Technology Provides Early Warning Systems

Wireless Systems Installed at Two Major Sites

by Laura Burns

Acoustic Technology, Inc. (ATI Systems) designs, manufactures and installs emergency warning and notification systems for the campus, community, industrial and military markets. Incorporated in Massachusetts in 1981, ATI Systems developed a wireless system that provides audible and visual warnings via a simple and compact hardware design, user-friendly software and the latest advances in communication methods, including radio frequency, IP Ethernet and satellite technology. The cases below highlight two ambitious projects that ATI has worked on recently.

INDIAN POINT ENERGY CENTER

ATI Systems was selected to provide a complete emergency warning system for the 10-mile Emergency Planning Zone (EPZ) surrounding the Indian Point Energy Center in Buchanan, NY. Operated by Entergy, Indian Point is a nuclear facility on the east bank of the Hudson River with unique safety requirements mandated by the *Energy Policy Act* of 2005 and the US Nuclear Regulatory Commission. Indian Point needed a reliable system to alert the public in case of any emergency that could affect the surrounding communities. ATI Systems' extensive installation is one of the largest mass notification

ATI Systems

ATI system at the World Trade Center Site

…the first state-of-the-art siren system in the country to use redundant communication paths and control points for system communication.

systems in the world, covering four New York counties and a wide geographic area. The ATI system will provide audible alert tones and intelligible voice commands in certain areas via its outdoor speaker system in case of any hazardous event requiring immediate action.

ATI Systems designed, manufactured and installed a unique, complete, CAP-compliant system[1] using its proprietary acoustic model to ensure audibility throughout the entire EPZ surrounding Indian Point Energy Center. This is the first state-of-the-art siren system in the country to use redundant communication paths and control points for system communication. It was approved by the Federal Emergency Management Agency (FEMA) for use in August of 2008.

The System includes 11 Control Stations (CS) for activating, (silent) testing and monitoring the alerting units with fully functional tone alert, and live and pre-recorded voice messaging capabilities. Two of the CS are located at the Indian Point Energy Center and are capable of controlling the entire system, including the simulcast communication system. Each county controls its own alerting units through two (or three in the case of Westchester County) strategically-placed CS. Each county can also


ATI Systems

monitor the status of neighbouring counties' CS. In the event of failure of one of the CS, authorized personnel from surrounding counties can activate the other alerting units.

WORLD TRADE CENTRE

The Port Authority of New York and New Jersey's reconstruction of the World Trade Centre (WTC) complex is underway with ambitious plans for five new skyscrapers, a memorial park and museum, a new transportation hub, a retail complex and a performing arts centre. The safety and security of the construction and planning team are paramount. Therefore, in September 2008 ATI Systems was awarded the contract to provide an emergency warning system at the construction site. The ATI system will provide audible alerts and intelligible voice commands through its outdoor speaker system. In case of any hazardous event, weather-related or man-made emergency that requires an evacuation or relocation from the various construction zones within the site, the ATI system will immediately notify the construction and planning team.

ATI Systems designed and manufactured a complete system and installation is now underway. The system design is based on the company's proprietary acoustic model, which will ensure sound audibility and voice intelligibility throughout the entire construction site with minimum echo and reflection. Sound will be projected into the site from the perimeter rather than from the centre outward to achieve a minimal amount of sound disruption to the neighbouring community. The mass notification system meets all applicable code and standard requirements and has field-proven reliability. Its user-friendly software interface will be operated by the Port Authority police and authorized staff to ensure the safety of the WTC construction community through each phase of the reconstruction project, which is expected to continue through 2013. Once construction is completed, the ATI system can be expanded to interface with other emergency notification solutions, such as text messaging and desktop alerting, to continue to ensure the safety of the WTC complex in both outdoor and indoor locations.

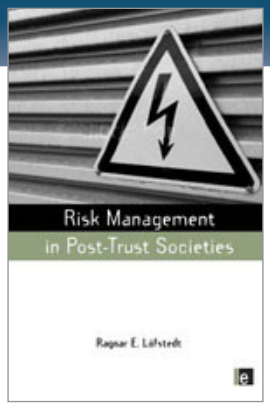
ATI Systems conducts work throughout Canada and has recently been awarded a contract with Queen's University, Kingston. ATI will be present at the International Association of Campus Law Enforcement Administrators in Quebec City, June 20-23, 2009.

Laura Burns is Vice President at ATI. For further information about ATI Systems, please contact Timothy Byrne, tim@atisystem.com, 617-567-4969 x226.

[1] Common Alerting Protocol (CAP)

BOOK Review

by Elisa Obermann



Risk Management in Post-Trust Societies

by Ragnar E. Löfstedt
Hardcover edition published by Palgrave Macmillan in 2005 (ISBN 9781403949783)
Paperback edition published by Earthscan in 2008 (ISBN 9781844077021)

The rise of the internet and 24/7 media coverage has led to greater scrutiny of government regulations and their failings. This scrutiny has contributed to a growing skepticism about political parties and actors and the efficacy of the public services for which they are responsible. Trends are clear: public trust in government is declining. This decline in trust in government is generally considered an obstacle for effective risk management and communication strategies for public agencies.

In *Risk Management in Post-Trust Societies*, Ragnar Löfstedt questions this conventional wisdom. He argues that successful risk management may not in fact be about achieving high levels of public trust. Rather, successful risk management may depend on how policy-makers interpret and manage existing levels of trust.

Löfstedt details a number of cases to demonstrate that there is no "one size fits all" solution in risk management. He examines in rich detail four cases: the decision to locate a waste incinerator in Germany; the relicensing of a privately owned US hydro-dam; the management of a nuclear power plant in Sweden; and the disposal of an oil storage buoy off the coast of the UK in the North Sea. In each case, Löfstedt analyzes how policy-makers' assumptions about public trust have considerable effect on the outcome.

Löfstedt challenges the notion that deliberative democracy and stakeholder dialogue are necessarily the best ways to proceed in such cases. Löfstedt posits three 'ideal types' of risk management strategy: deliberation (stakeholder participation and dialogue), technocracy (expert opinion, technical solutions) and rational (cost-benefit criteria). Löfstedt explains that the three possible components of trust—fairness, competence and efficiency—should dictate which of the three strategies policy-makers should adopt. For example, in a high-trust/uncertain risk situation, Löfstedt suggests that a top-down, technocratic approach is appropriate. Given the high level of trust, the public may already view the regulatory system as fair, competent and efficient, and therefore capable of making suitable decisions. If, on the other hand, the public is asked to participate in a deliberative policy-making process, the public could become more suspicious or weary of the regulator's competence and efficiency. Ironically, this effort to open up the consultative process could in fact decrease public trust in the regulator. In contrast, a deliberative approach might be appropriate in climates of high public *dis*trust, which may be fuelled by the idea that regulators are unfair or partial. This approach allows citizens to feel that their voices are being heard.

> …successful risk management may depend on how policy-makers interpret and manage existing levels of trust.

Löfstedt's approach is not foolproof. The risk management and communication methods and tools he presents can still be hindered by funding constraints, established regulatory processes and/or lack of political support, for instance.

Still, the book is largely successful. While it is clear that Löfstedt challenges the wide use of deliberation, he essentially draws our attention to the fact that each case is situated in a slightly different context, which policy-makers should consider. Moreover, Löfstedt provides an accessible and comprehensive account of how trust can be re-established through the strategic choice and use of risk management tools and methods. He also presents a risk management decision tree that policymakers can apply not only to implement risk management strategies but also to gain a greater understanding of public trust. The decision tree is not overly prescriptive, however. Rather than viewing risk management as a problem that can be solved with textbook answers and solutions, Löfstedt recognizes that each problem requires a slightly nuanced approach.

Elisa Obermann is a recent graduate of Dalhousie University's Master of Public Administration program.

Trust and CIP

Kevin Quigley

The concept of trust is cited frequently in most governments' CIP strategies. Governments seek to develop trusted relationships with and between CIP stakeholders in the public and private sectors to facilitate—among other things—the exchange of sensitive information about vulnerabilities. There is evidence that suggests trust improves organizational effectiveness by increasing group cohesion.[1] Unfortunately, there is also evidence that trust generally is in decline. Seventy-five percent of Americans, for example, said they trusted the government in 1964; only 25% expressed comparable levels in 1997. Private organizations—the owners and operators of most of the critical infrastructure—fare no better than government agencies: trust in private institutions fell from 55% to 21% over the same period.[2]

What is Trust?

Although social scientists have given considerable attention to the problem of defining trust, a concise and universally accepted definition remains elusive. As a consequence, the term trust is used in a variety of distinct and not always compatible ways in organizational research.[3] Barbelet argues that trust is often confused with consideration of legitimacy or loyalty, for instance. He contends that trust must be understood in terms of (a) acceptance of dependency in (b) the absence of information about the other's reliability in order to (c) create an outcome otherwise unavailable.[4]

Generally, there are two broad tendencies in definitions of trust.[5] At one end of the spectrum are formulations that highlight the strategic and calculative dimensions of trust in organizational settings. We will call this the rational actor approach. It draws largely from economics and political science. Viewed through this lens, individuals are expected to maximize expected gains or minimize expected losses from their transactions. Within this tradition, two elements are critical to understanding the potential for trust. The first element is the knowledge that enables one person to trust another. The second is the private incentive that exists for the person to honour and fulfill that trust. This approach is often criticized for being too narrowly cognitive; it gives too small a role to emotional and social influences.

The second broad approach to trust derives from relational models, which consider social orientation to other

people and society as a whole. We will call this the socio-cultural approach. A common feature of this approach is the focus on social rather than merely instrumental (resource-based) motives driving trust behaviour. Most in this tradition agree that trust is a multi-dimensional concept that reflects an interaction of values, attitudes and other socio-cultural references.[6]

Conditions Necessary for Trust

Within this second tradition, there is also no standard definition of trust and therefore no set list of qualities that are required in order to create a setting that is conducive to trust-building.

[1] Jeffcott, S., Pidgeon, N., Weyman, A. and Walls, J. (2006) "Risk, Trust, and Safety Culture in U.K. Train Operating Companies." *Risk Analysis*. 26:5.
[2] Kramer, R. M. "Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions." *Annual Review of Psychology*. 50: 569-598.
[3] IBID
[4] Barbelet, J. (2006), "A Characterization of Risk and Its Consequences." *Social Contexts and Responses to Risk Network*. 2006/13.
[5] There are other ways to think about trust. Kramer (1999; noted above) also notes *history-based trust*, which characterizes trust as something that evolves over time and is based on past experiences with individuals, *category-based trust*, which is based on membership, and *roles-based trust*, which is based on one's place or formal authority in an organization.
[6] Jeffcott, S., Pidgeon, N., Weyman, A. and Walls, J. (2006) "Risk, Trust, and Safety Culture in U.K. Train Operating Companies." *Risk Analysis*. 26:5.

That noted, there are some trends in the literature. Peters, Covello and McCallum identified three dimensions that people tend to look for in others to develop trust:[7]

1. knowledge and expertise;
2. care and concern; and
3. openness and honesty.

Medical doctors and natural scientists, for example, tend to rank highly in all three categories, which is why they tend to be highly trusted.

The concept of open communication, in particular, appears repeatedly in research on developing organizational trust[8] and is said to encompass free data-sharing, inclusive decision-making and collaborative working.[9]

Why is it difficult to achieve and maintain trust?

Trust comes on foot but leaves on horseback, Calman notes.[10] Trust is easy to lose because negative information that can diminish people's feelings of trust is more attention grabbing, more powerful and often more readily available than positive information.[11]

There are also a number of broad social trends that seem to be incompatible with developing trust. Public sector reform has tended towards market-driven or -inspired solutions. Crucially, the stress on competitive and consumerist logic may undermine a core component of (socially constructed) trust, since the motivation of providers is declared to be self-interest, in response to market signals, rather than public interest.[12] In Jeffcott *et al.*'s study of post-privatization British railways, they noted that fragmentation, performance regimes, procedurralization, loss of expertise and major accidents all affect trust relationships across industry.[13]

> …the complexity and interdependence of the networks make knowledge and certainty elusive concepts.

How does this relate to CIP?

If governments assume the rational actor approach to generating trust, the model should work provided government's interests are aligned with industry interests as well as with broader social ones. Indeed, there are many instances in emergency planning generally in which this is the case. One can imagine instances, however, in which these parties' incentives may not be aligned. For instance, while governments may wish to obtain information about vulnerabilities in the infrastructure in order to mitigate the risk of cascading failures, owners and operators of critical infrastructure may be reluctant to disclose the vulnerabilities of their assets because of the risk to their organization's security, liability, share value and public image. There are other challenges. Governments might like industry to take a more proactive stance by adopting certain risk management practices, which industry might see as an unnecessary drain on much needed resources, particularly in tough economic times.

If one assumes the socio-cultural understanding of trust, solutions are not necessarily any easier. None of the three conditions identified above—knowledge, care and openness—is readily achieved in CIP, for instance. To start, the complexity and interdependence of the networks make knowledge and certainty elusive concepts. Even care and concern might be difficult to achieve. Sato (in a different context) concluded that the effects of trust *weakened* as group size increased;[14] participants feel their impact is less in larger groups, which arguably leads to

[7] Peters, R.G., Covello, V. T. and McCullum, D. B. (1997), "The Determinants of Trust and Credibility in Environmental Risk Communication: An Empirical Study." *Risk Analysis.* 17 (1), as cited in Eiser, J. R. and White, M.P. (2006), "A Psychological Approach to Understanding how Trust is Built and Lost in the Context of Risk." *Social Contexts and Responses to Risk Network.* Working Paper 2006/12.
[8] Clarke, M. C. and Payne, R. L. (1997), "The Nature and Structure of Workers' Trust in Management." *Journal of Organizational Behaviour.* 18.
[9] Firth-Cozens, J. (2004), "Organizational Trust: The Keynote to Organizational Safety." *Quality of Safety and Health Care.* 13 and Jeffcott, S., Pidgeon, N., Weyman, A. and Walls, J. (2006) "Risk, Trust, and Safety Culture in U.K. Train Operating Companies." *Risk Analysis.* 26:5.
[10] Calman, K. C. (2002), *"Communication of Risk: Choice, Consent and Trust." Lancet. 360.*
[11] Eiser, J. R. and White, M. (2006), "A Psychological Approach to Understanding how Trust is Built and Lost in the Context of Risk." *Social Contexts and Responses to Risk Network.* Working Paper 2006/12.
[12] Taylor-Gooby, P. (2006), "The Efficiency/Trust Dilemma in Public Policy Reform." *Social Contexts and Responses to Risk Network.* Working Paper 2006/9.
[13] Jeffcott, S., Pidgeon, N., Weyman, A. and Walls, J. (2006) "Risk, Trust, and Safety Culture in U.K. Train Operating Companies." *Risk Analysis.* 26:5.
[14] Sato, K. (1988), "Trust and Group Size in a Social Dilemma." *Japanese Psychology Research.* 30.

a sense of helplessness rather than one of care and concern. Finally, government also faces a trust/transparency conundrum. On the one hand, researchers have noted that 'open communication' is a prerequisite to organizational trust. On the other hand, too much transparency might make owners and operators of the critical infrastructure nervous about disclosing information about vulnerabilities to government.

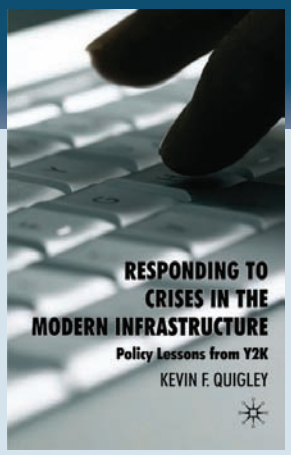
Wither the trust, wither the CIP? While it may be a setback, it may not be cataclysmic. In his book *Risk Management in Post-Trust Societies* (reviewed on page 14) Löfstedt notes that different levels of trust require different approaches. What is important is to understand the context in which one is acting, and then adopt an appropriate solution.

While most governments refer to trusted partnerships, in many cases they may actually be referring to dependencies.[15] Does government wish to be seen as a trusted 'partner' in this context? It certainly has advantages: in the right context it can generate stable and collegial relationships, which can be crucial in emergency planning. Interest group theory would caution, however, that stable and collegial relationships can also prevent dramatic change (when needed) and limit transparency.

In any event, pursuing 'trust' as some sort of Holy Grail may also result in *misplaced* trust. Government has a regulatory role to play. By sitting at a round table as a partner, government potentially compromises its capacity to play the role of enforcer. Indeed, forging reasonable standards backed by a strong audit function and appropriate incentives might align industry interests with those of government more effectively, while at the same time generate a context for a strategic dialogue between government and industry on CIP.

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

[15] Please see CIP panel discussion on June 3, 2008, at www.cip.management.dal.ca for further discussion on this point.



Kevin F. Quigley
Responding to Crises in the Modern Infrastructure: Policy Lessons from Y2K
Published by Palgrave Macmillan

New Book from the Editor

In a 1996 letter to President Clinton, Senator Pat Moynihan wrote, "the computer has been a blessing; if we don't act quickly, however, it could become the curse of the age." The Senator was commenting on a date-generated computer bug that became known as Y2K (Year 2000). President Clinton would eventually describe it as "one of the most complex management challenges in history." Margaret Beckett, Chair of the British Cabinet Committee on Y2K, would describe the UK government's response to it as "the largest co-ordinated project since the Second World War." The US government and UK government spent billions on preparations. And, in the end, virtually nothing happened. Did this mean success? Despite the scope and cost of Y2K it has received almost no critical analysis, academic or otherwise, since it occurred.

This book examines comparatively the US and the UK governments' management of Y2K and considers the extent to which such management can be understood as responses to market pressures, public opinion and organized interests. It concludes by providing valuable lessons to those concerned about managing risk and critical infrastructure today.

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:
CANADA SCHOOL OF PUBLIC SERVICE