THE CIP EXCHANGE

Cyber-Security and Supply Chain *Edition*

A forum for sharing views and information about critical infrastructure protection

SPRING 2014

Contents

Editorial

Editor: Kevin Quigley / kevin.quigley@dal.ca

Copy Editor: Janet Lord

Design: Dalhousie Design Services

Additional Thanks: Ron Pelot and Colin Macdonald

DALHOUSIE UNIVERSITY
Inspiring Minds

Faculty of Management

School of
Public Administration

cip.management.dal.ca

Peers for fears

Peer networks help to distinguish between viable threats and exaggerated claims in cyber-security, researchers note

BY COLIN MACDONALD

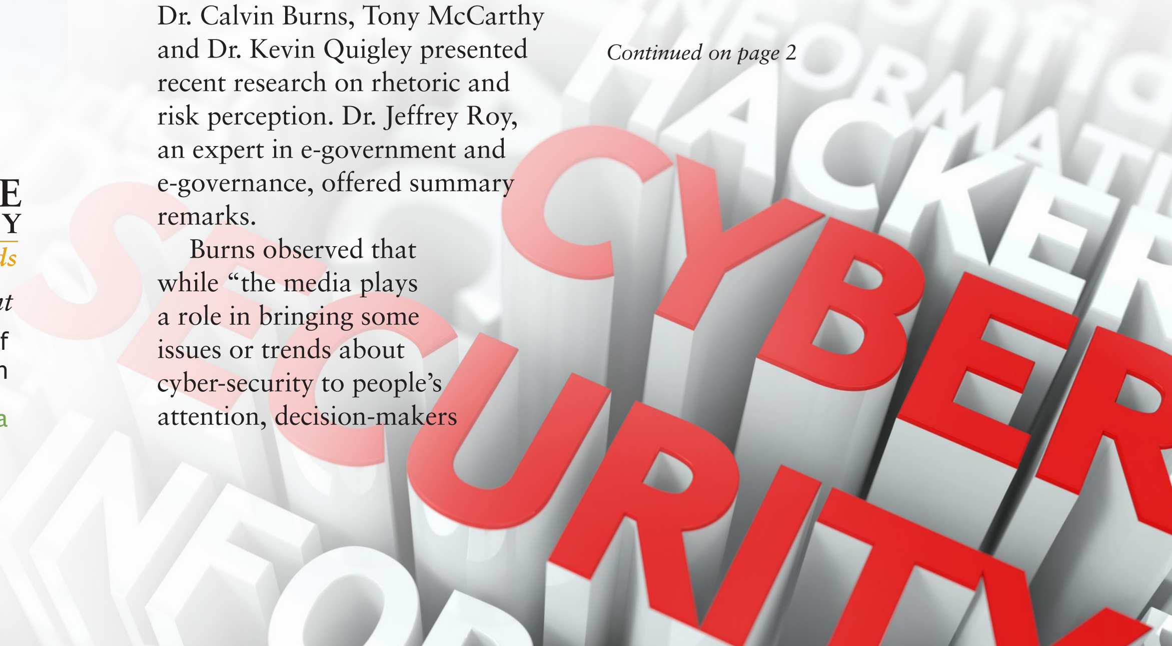
TONY MCCARTHY, A PHD candidate from the University of Strathclyde, explained that people often perceive rare cyber risk events as more imminent threats, largely due to hyperbolic media reports and a poor understanding of cyber-security. He noted that perception of risk in cyber-security is correlated with that person's level of trust in the organization managing it.

These were among some of the observations on June 19, 2013, at the CIP Initiative's third in a series of five transatlantic workshops in the immersive online technology *Second Life*. The subject of this workshop was risk communication and cyber-security. Dr. Calvin Burns, Tony McCarthy and Dr. Kevin Quigley presented recent research on rhetoric and risk perception. Dr. Jeffrey Roy, an expert in e-government and e-governance, offered summary remarks.

Burns observed that while "the media plays a role in bringing some issues or trends about cyber-security to people's attention, decision-makers in public sector organizations tend to be influenced most by peer networks." He also noted that these same decision-makers are generally less concerned with terrorism and sabotage and more concerned with the loss or theft of private data. He highlighted the importance of risk communication in risk management and recommended that governments continue to recognize and support peer networks in managing cyber risks.

Reporting on recent research conducted with Kristen Stallard, K. Quigley explained that the popular media, such as magazine articles or TED talks, rely to varying degrees on metaphors, hyperbole and anecdotal evidence

Continued on page 2



Peer for fears *continued*

when communicating about cyber threats. Media use war imagery and zombie metaphors and create elaborate (hypothetical) scenarios in which hackers attack critical infrastructure. These 'cyber gurus,' however, rarely provide empirical evidence of these types of attacks.

Roy concluded the session by noting that this research is timely and much needed because risk probabilities are typically overlooked; potential consequences often fuel the debate. Due to a lack of transparency, it is difficult to tell how real these threats are. He also remarked that definitions of cyber-security are too varied, vague and broad to be useful. "The macro-challenge for government will be in defining and framing the debate," he added, noting that collaboration through peer networks can help to develop a common definition. He cautioned, however, that the tension between secrecy and openness can undermine efforts to establish trust, which is essential to the success of peer networks.

This workshop was made possible by a SSHRC-funded partnership development grant. The goal is to develop risk networks that include academics, practitioners and government. The workshop was chaired by Dr. John Quigley from the University of Strathclyde. For more information on this workshop, please visit our website.

Colin Macdonald is coordinator and research analyst for the CIP Initiative at Dalhousie University.
E-mail: colin.macdonald@dal.ca

The CIP Initiative publishes report on Canadian transportation security

In February 2014, the CIP Initiative published *An Analysis of Transportation Security Risk Regulation Regimes: Canadian Airports, Seaports, Rail, Trucking and Bridges* by Dr. Kevin Quigley and Bryan Mills.

This report is the first in a series of three. The second report will examine the risk regulation regime in Canada that governs major incidents involving dangerous chemicals and the third will examine the Canadian risk regulation regime that governs critical infrastructure in the agricultural sector. A draft of the paper on dangerous chemicals will be on the website shortly. The report on the agricultural sector will follow later this year.

These reports have received support from the Kanishka Project Contribution Program. The Program is a multi-year investment in terrorism-focused research funded by the Government of Canada. Its primary focus is on research, but it also supports other activities necessary to build knowledge and create a vibrant network of researchers and students that spans disciplines and universities. Through this project, the government is funding policy-relevant projects that will improve understanding of terrorism in the Canadian context, how that is changing over time, and how policies and programs can best counter terrorism and violent extremism in Canada (Public Safety Canada, 2013).

Reference:

Public Safety Canada (2013). Second round of successful Kanishka Project Research Proposals. Retrieved from: http://www.publicsafety.gc.ca/cnt/nws/nws-rlss/2013/20130228-1-eng.aspx

The CIP Initiative is publishing three articles on Canadian critical infrastructure security:

Transportation sector – Available on our website

Dangerous chemicals sector – Coming in the fall

Agriculture sector – Coming in the winter

Interview with Paul Stockton

Paul Stockton discusses cyber-security, insider threats, finding a balance between efficiency and security and protecting the rights of citizens

BY KEVIN QUIGLEY

DR. STOCKTON IS THE FORMER Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs. He is currently the President of Cloud Peak Analytics and Managing Director, Sonecon, llc. He holds a PhD from Harvard University. Kevin Quigley interviewed Dr. Stockton on August 1, 2013.

KQ: What are the biggest threats to critical infrastructure in North America today?

PS: Interconnectedness and the risk of cascading failure of critical infrastructure, regardless of the cause. This is especially so for infrastructure with single points of failure—those without redundancy. The consequences of adversaries using kinetic (physical) attacks combined with cyber are significant. For example, if there should be, as former Secretary of Defense Panetta called it, a cyber–Pearl Harbor attack on the electric power grid, interconnected infrastructure would very quickly begin to feel the effects. While many of these critical infrastructure components have back-up power generators, the problem is that those generators can only operate for so many hours with fuel stored onsite. As we learned during Hurricane Sandy, those generators, if run too long, can catch fire or unexpectedly stop functioning. Cascading failure of critical infrastructure can create a very difficult environment in which to conduct the lifesaving and infrastructure restoration activities that are essential in Canada and the United States.

Above all manmade threats, however, is the risk of insider attacks—when trusted employees in an infrastructure company introduce malware or otherwise interfere with operations. The events surrounding Mr. (Edward) Snowden highlight that personnel inside the security perimeter of a critical infrastructure company can create terrific harm. This is especially dangerous if such an attack were coordinated with other means of attack.

KQ: How do we make headway on insider threats?

PS: Well, the challenge of improving our security against insider threat is a constant battle. I had the honour of leading the effort in the U.S. Department of Defense after the 2009 shootings at Fort Hood to try to build better policies in the United States to deal with insider threats. There are many lessons to be learned from that effort, but I would emphasize the need in Canada and the United States for specific government agencies and private sector companies to build tailored approaches to these challenges of insider threats in a way that fully respects the rights of Canadian and U.S. citizens.

KQ: A common theme is the importance of sharing information to protect critical infrastructure, yet at the same time the insider threat reveals the risks associated with letting information flow too freely. How do you strike that balance?

PS: You've highlighted the devil's bargain. Web-based controls and information-led operations in critical infrastructure create increased connectivity and terrific efficiencies, but bring with them new vulnerabilities, both from insiders and those who would attack from outside the perimeter.

KQ: Cyber-security is an area that does not always resonate with the public. How do we bring the public along with us in cyber-security?

PS: I believe that universities have a responsibility to make sure citizens are aware of what's at stake for the economy, for public health and safety, and ultimately for national security when we look at the emerging threat of cyber-attack in critical infrastructure. The security community must continue to reach out to industry partners so that there can be a shared approach to raising awareness of these challenges, while also always keeping in the forefront the need to protect the rights of citizens.

Risk perception, trust and affective judgement in cyber-security

BY TONY MCCARTHY

THE INCREASED USE OF information technology and the Internet has led to an ever greater and increasingly complicated problem of cyber-security. Despite this, evidence suggests that the issues relating to cyber-security are poorly understood. Largely as a product of media exaggeration, many people tend to perceive relatively rare risks (such as cyber-terrorism) as imminent threats (Hansen & Nissenbaum, 2009). Terms such as ‘electronic weapons of mass disruption’ have played on the emotional reaction they elicit. This is despite a lack of empirical evidence to support such fears (Hansen & Nissenbaum, 2009; Cavelty, 2007).

This issue of fear driving risk perception can be understood in terms of the ‘affect heuristic’ (Slovic et al., 2007). This theory suggests that emotion (or affect), particularly negative emotion, is often a driver for risk perception. Specifically, that negative emotional reaction is associated with high risk, and vice versa. This also relates to the conceptualisation of risk perception as existing along the two dimensions of ‘dread’ and ‘unknown’ (Slovic, 1987). This theory suggests that the extent to which the risk generates dread, and how much the risk is known (familiar or understood) determines the eventual perception.

This study investigated the impact of emotion (or affect) and also how the ‘unknown’ dimension may impact perception. Specifically, this second part was in relation to perceptions of organizations. The ‘Trust Determination Theory’ suggests that people need to feel a source of information exhibits appropriate attributes, such as competency, commitment, honesty, and empathy (Covello, et al., 2001). Subjects in the study rated cyber-security terms and cyber companies, with the aim of determining what associations to affect and trust were evident.

Subjects / Method

There were 43 subjects with 20 male, and 23 female. The ages ranged from 21 to 60, with a mean age of 27 (*SD* = 7.3). All subjects were postgraduate students who were entered in a raffle for participating.

Surveys were disseminated online via the web resource Qualtrics. On-screen sliders were used as the tool for the judgements, using a scale

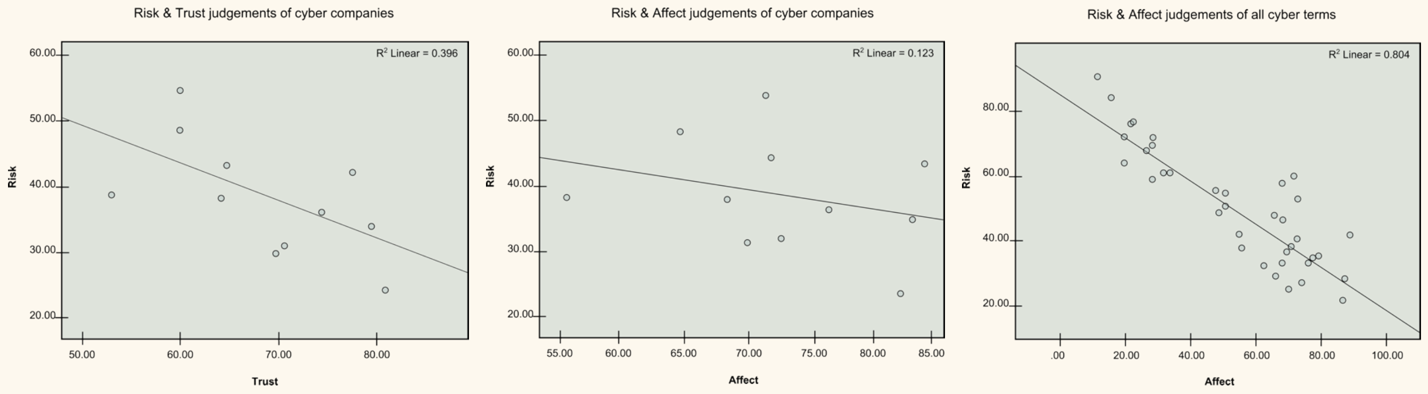


Figure 1: Scatterplots for the by-items analyses. From left to right, Risk and Affect judgements for all terms (basic terms and companies together), Risk and Affect judgements for cyber companies, and Risk and Trust judgements for cyber companies.
All scatterplots include the line of best fit.

Risk perception, trust and affective judgement in cyber-security *continued*

of 0-100. After asking for demographic information (e.g. age and gender), subjects were asked to rate a series of words for Risk and Emotion (Affect). They made their ratings by moving a slider on the screen between the extremes of High Risk / Low Risk, and Positive Emotion / Negative Emotion. The judgements were based on the associations the subject considered appropriate for each term. The judgements were made for a series of 26 cyber related terms (e.g. virus, firewall), and also a selection of 11 cyber related companies (e.g. Apple, Google). The companies were rated for Trust along with Risk and Affect.

Results / Discussion

Initial by-subjects analyses were conducted to determine if there were any age or gender effects. No significant effects were found (all $p > .11$). The main analyses were conducted by-items using Pearson correlations.

When analysing all items (terms and companies together), there was a significant correlation between Risk and Affect judgements, $r(35) = -.897$, $p < .001$. This shows that as Risk is judged higher, Affect denotes increasing negative appraisal.

For the companies only, there was a significant correlation between Affect and Trust, $r(9) = .939$, $p < .001$. This shows that as Affect is judged more positively, the companies are also judged as more Trustworthy. Trust was also significantly correlated with Risk, $r(9) = -.629$, $p = .038$, showing that as Trustworthiness increases, Risk is judged as lower. There was no significant correlation for Risk and Affect, $r(9) = .35$, $p = 291$. See Figure 1 for scatterplots.

The results are largely in line with previous research (e.g. Slovic et al., 2007). High risk was associated with negative affect, and low risk with positive affect. This showed a linear relationship, such that as the risk decreased, the affective judgement gradually tended to be more positive. This is an important distinction to much of the previous research which has tended to focus on extreme ratings. This study also suggests that the influence of affect is not mainly restricted to negative emotion, but is similarly evident for positive affect. As such, future research would benefit from a holistic approach to the impact of emotion on risk perception.

It should be noted that the impact of affect was only evident for the terms (e.g. virus, firewall). When rating the organizations (e.g. Apple, Google) it was trust that showed a significant association, with no such association for affect. This is in line with the ‘Trust Determination Theory’ and appears to show that when judging a group, it is trust that determines the perception. This suggests that an organization will not necessarily be able to influence risk perceptions of its messages by judicious use of the affective component. Rather it is the extent to which it is trusted that is likely to influence perception, and this may depend on factors such as competence, rather than affect. It should be noted, however, that trust and affect are arguably related. This study certainly showed a strong association between them. This may suggest that the processing involved for the terms and the companies is similar, but conceptualised differently by the perceiver. Future research could attempt to determine if this is the case.

References

Cavelty, M. D. (2007). Cyber-terror: Looming threat or phantom menace? The framing of the US cyber threat debate. *Journal of Information Technology and Politics*, 4(1), 19-36.

Covello, V. T., & Sandman, P. M. (2001). Risk communication: Evolution and revolution. In A. Wolbarst (Ed.), *Solutions to an Environment in Peril* (pp. 164-178). John Hopkins University Press.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, 53, 1155-1175.

Slovic, P., Finucane, M., Peters, E., & Macgregor, D. (2007). The affect heuristic. *European Journal of Operational Research, 177*(3), 1333-1352. doi:10.1016/j.ejor.2005.04.006

Slovic, P. (1987). Perception of risk. *Science, 236*(4799), 280-285. doi:10.1126/science.3563507.

Tony McCarthy is a PhD candidate in the Department of Human Resource Management at the University of Strathclyde Business School. He is studying risk perception and risk communication.
E-mail: joseph.mccarthy@strath.ac.uk

Interview with Thomas Rid

Thomas Rid, author of *Cyber War Will Not Take Place*, discusses the use of metaphors in cyber-security and the importance of distinguishing between 'good' and 'bad' subversion

BY KEVIN QUIGLEY

THOMAS RID, PHD, IS READER in War Studies at King's College London. From 2003 to 2011, he worked at leading think tanks and universities in Berlin, Paris, Washington and Jerusalem. Rid has published four books and numerous scholarly articles on international security, the history of strategy, political violence, deterrence and new technologies.

KQ: In your recent book you argue *Cyber War Will Not Take Place*. Why?

TR: Cyber war has become a chimera, a myth. Almost always when somebody talks about 'cyber war'—a journalist, a politician, a military officer, an IT specialist—they do not bother defining what they mean. I tried doing so in my book. And since I'm at the Department of War Studies at King's College London, one of the oldest and biggest institutes studying conflict in all its shapes and forms, I used classic strategic thought. We can't discuss war in a vacuum. The most pithy definition of war is from Carl von Clausewitz's book, *On War*: the Prussian thinker defined war as an act of force to compel the enemy to do one's will. This sentence contains all critical elements: force, or violence (Clausewitz used Gewalt in German); instrumentality (using force as a means, not as an end on its own); and a political intention (in a cyber-security context that translates into claiming credit for an attack). No cyber attack meets all of those criteria. Very few meet even one.

KQ: You analyze cyber threats using Carl von Clausewitz's traditional definition of war. Why is it important to analyze cyber attacks using this definition?

TR: We have to use some kind of framework to analyze human behaviour. That of course includes violent human behaviour, and even war. Those who think they don't need a framework are still using one without noticing it. So I'd rather make mine explicit, so we can have a proper argument: Clausewitz offers an excellent starting point—the best I've seen.

Sometime critics of the argument say that my view of violence is too narrow. That the loss of intellectual property and economic competitiveness amounts to violence, perhaps to some form of structural violence. Or that breaching a network can be some form of violence. They say: we need to update our notion of violence for the 21st century, to which I would respond: OK, then deliver the goods. But I haven't seen many sensible suggestions yet.

Losing data can be traumatic. Say someone deletes all of your company's data, irretrievably, or someone loses all their email and, God forbid!, their Facebook account with all contacts. Such a loss can affect one's personal wellbeing, certainly. But still, suffering a severe physical injury as a result of a violent attack, say the loss of one or both legs in an IED explosion, is certainly in a different category. The victim encountered the possibility of death, not in the abstract, but in the concrete. Physical attacks can quickly turn existential; cyber attacks do not. Violence demands respect.

Interview with Thomas Rid *continued*

KQ: Metaphors are often used to relate complex issues to those without the knowledge or experience to deal with the technical aspects of the issues. In your book, you take exception to the metaphors we currently use to describe the security of the Internet. What kind of metaphors should we be using when explaining Internet security issues?

TR: That depends on the issue at hand, I suspect. All metaphors are imperfect. The important thing is to see the didactic benefit of metaphors—they help explain complex aspects—but at the same time see the point of failure. Take 'firewall'; many people without a technical background will think, "Oh, I've got a firewall, I'm safe." But it all depends on the firewall's configuration. You don't need to configure a firewall made of asbestos or steel.

KQ: A review of your book by the *Financial Times* argues that "the world is full of examples of sporadic attacks used as coercive tools, nearly always attributed, directly or indirectly, to a state–but with some uncertainty and usually after a lag" and cites some examples (e.g., North Korea sinking a South Korean ship). How do you respond?

TR: There are two noteworthy things here. It's one thing if something is 'attributed' by a third party days or weeks or months after the fact; it's quite different to claim credit for an attack as it happens, as in, "I am doing this to you." So far, states don't tend to claim credit for cyber attacks. Second, clandestinely sabotaging something is not necessarily coercive. Coercion means you try to change somebody's decision, their will to act; sabotage often means you're merely messing with your opponent's means to act.

KQ: Should governments in the West assume a more aggressive regulatory stance on the security of IT operated by the owners and operators of critical infrastructure?

TR: It depends on the sector, on how critical the infrastructure is. I'm very skeptical of wholesale regulation. But specific regulation, especially when it comes to documenting system requirements, can be very effective. I'd like to point out that vendors also have responsibility, not just operators and owners.

KQ: After the Snowden NSA leaks, polls showed that Americans were somewhat complacent about the idea of having their online activity monitored. Are people reconsidering the balance between privacy and security, if indeed there is a tension? What are the medium-term implications?

TR: Intelligence agencies in all countries are under tremendous pressure to adapt to 21st century communication trends and technologies. In some ways non-democratic countries have it easier: for them, all subversive activity is bad subversive activity. That's different in democracies and capitalism, where a degree of subversion is considered necessary for political and economic renewal. Open democracies therefore need to have a discussion on where and how to draw the line between liberty and security, between 'good' subversion and 'bad' subversion. That discussion has now started in earnest, and that's a good thing.

KQ: Since 9/11, governments have encouraged a freer exchange of information among trusted parties to ensure more effective responses to protecting critical infrastructure. At the same time, and as you acknowledge in your book, security lapses in critical infrastructure often require 'insiders.' How does government manage the tension between sharing information and guarding against the insider threat?

TR: The insider threat is complex. Only sophisticated security setups can avoid insider attacks. If a truly critical modification requires only one rogue insider, then there's a risk. If it requires two or even three people to provide verification credentials, the risk goes down. The insider threat, like so many security issues, is problem of trust.

Kevin Quigley is an associate professor and director at the School of Public Administration, Dalhousie University, and the principal investigator of the CIP Initiative.
Email: kevin.quigley@dal.ca

Cyber rhetoric

Researchers publish a report on cyber discourse in popular and academic publications

BY KEVIN QUIGLEY, KRISTEN STALLARD AND CALVIN BURNS

MUCH OF THE RESEARCH ON computer security, information technology and supply chain management focuses on the ways in which organizations secure their networks and information in the supply chain. Less attention has been paid to how organizations construct and understand cyber risks, as well as to how this framing impacts their approach to managing cyber risks. Our study seeks to address some of these gaps in the existing cyber-security literature.

There are several stages to our analysis. We are particularly interested in using the 'management guru' literature and the risk psychology literature to examine how present-day cyber gurus describe security risks associated with information technology.

Cyberspace as 'Battlefield' is a common metaphor

What We Did

We selected ten samples in total from a variety of sources, including the popular media, commercial books and academic publications. The authors of these pieces come from diverse fields, representing politicians, public servants, journalists, CEOs, academics and computer scientists. All pieces were published between 2010 and 2012, and come from American, British and Canadian sources. Additional comments about the method can be found in the final report.

What We Found

The analysis found that the samples align with many of the predictions of the literature. Many of the samples confuse and conflate key terms such as cyber-terrorism with the more probable 'hacktivism' and cyber-crime. The availability heuristic—mental shortcuts that we use to estimate the probability of events by how easy it is to think of examples—was found to be at play in the way that the samples create associations between technology and catastrophic events like terrorist attacks. In sum, the samples neglected probabilities, emphasized conventional war-like catastrophic outcomes and provided only limited advice on how to address the risks.

There are some important concessions. While the authors of the selected pieces rarely provide empirical data to support their claims, in fact, terrorism information is not always readily available. Private organizations, for example, do not necessarily report breaches of their security lest they expose weaknesses in their security infrastructure. As such, reliable information on the frequency and severity of attacks is not always easy to come by. The issues with transparency in this field make it challenging to verify claims made by cyber-gurus.

Nevertheless, while uncertainty still exists about threats to cyber-security, our findings raise serious questions about the potentially narrow manner in which security problems are framed.

Cyber rhetoric . . . *continued*

The authors rarely provide empirical data and do not reflect on the opportunity cost of extensive security practices.

Critical infrastructure is typically described as interdependent and vulnerable

Concluding Comment

With rapid advancements in technology, it is difficult for laypeople to make sense of emerging IT issues, opportunities and threats. There is a great deal of information asymmetry between laypeople and the technical experts who sell cyber-security solutions to individuals, businesses and governments. The benefit of this study is that consumers, businesses and governments will have more information at their disposal to assess the soundness of cyber-guru claims. Inquiring within peer networks is one way to address this problem. IT managers within organizations—both public and private—are in a position to offer a different and possibly more grounded perspective, thereby providing some balance to counter persuasive cyber-gurus.

The full paper can be found at cip.management.dal.ca

Calvin Burns is a lecturer in Industrial-Organizational Psychology in the Department of Human Resource Management at the University of Strathclyde.
Email: calvin.burns@strath.ac.uk

Kevin Quigley is an associate professor and Director at the School of Public Administration, Dalhousie University, and the principal investigator of the CIP Initiative.
Email: kevin.quigley@dal.ca

Kristen Stallard was a research assistant at the School of Public Administration, Dalhousie University, and now works at the Association of Municipal Administrators, Nova Scotia.
Email: kristen.stallard@gmail.com

Critical Infrastructure Protection
at Dalhousie

WHAT IS THE CIP INITIATIVE?

A national dialogue about how best to protect Canada's critical assets. It includes:

Panel events
Workshops
Second Life seminars

Don't miss what's critical. Join the dialogue today.

THE CIP EXCHANGE

Our publication, featuring:

Interviews with leading commentators
Research and event updates
Workshop proceedings
Book reviews and more

cip.management.dal.ca

Increasing food security through supply chain modelling

Workshop promotes the benefits of modelling uncertainty and resilience in supply chains

BY COLIN MACDONALD

Security specialist Gord Helm noted modelling complex supply-chain networks can identify weaknesses in network and prompt much needed scenario planning.

IN FOOD SECURITY, A MAJOR RISK event such as a natural disaster can shift government focus from food safety to food supply. A region's unique natural landscape can both inhibit and enhance recovery.

Mouhamad Shaker Ali Agha, a PhD candidate at the University of Strathclyde, spent four months studying risk in Atlantic Canada's food supply. Splitting his time between Dalhousie's Faculty of Engineering and the School of Public Administration, Ali Agha mapped and modelled the supply chain of a grocery retailer/supplier in the region.

Ali Agha noted the vulnerability of food supply chains to Newfoundland and the impact major natural hazards (e.g., hurricanes) could have on them. He used Bayesian Belief Networks (BBN) to show how failure at one point in the network can have a cascading impact. BBN, he concluded, can "enhance our ability to explore scenarios and predict possible futures."

On May 28, 2013, Ali Agha was joined by scholars and practitioners at the CIP Initiative's second in a series of transatlantic workshops in the immersive online technology *Second Life*. The subject of this workshop was supply chain resilience.

Echoing Ali Agha, Professor Lesley Walls and Dr. Robert van der Meer explained that the purpose of Bayesian Belief Network modelling is to capture the uncertainty that traditional engineering methods of risk modelling do not capture. This is accomplished through expert judgment and estimation of probabilities. They argue that by modelling the supply chain with Bayesian analysis, an organization can determine areas where small investments in flexibility increase resilience and, therefore, decrease risk of significant downtime.

Gord Helm, security expert and panel discussant, noted the benefits of modelling complex supply-chain networks. He remarked that the exercise can be a focusing event for organizations; it can force them to search for weaknesses in their network and prompt much-needed scenario planning. Often private organizations do not recognize their role in public infrastructure. Modelling resilience and identifying cost-effective methods of increasing flexibility and slack in their supply chains can help an organization's bottom line and increase public value, Helm noted.

The workshop was chaired by Dr. Ronald Pelot from Dalhousie's Faculty of Engineering. This was the second of five workshops Dalhousie and Strathclyde will co-host as part of a SSHRC-funded partnership development grant. The goal is to develop risk networks that include academics, practitioners and government. Each workshop will focus on a unique critical infrastructure challenge. For more information on this workshop, please visit our website.

Colin Macdonald is coordinator and research analyst for the CIP Initiative at Dalhousie University.
Email: colin.macdonald@dal.ca

Food supply network resilience in Atlantic Canada

BY MOUHAMAD SHAKER ALI AGHA

NEWFOUNDLAND IS A LARGE ISLAND off the east coast. Most wholesalers and grocers in Atlantic Canada have stores in Newfoundland, and in some instances a supplier of a particular good is located there; however, most goods must be imported. The only access is by boat or air and winter weather often impacts the transportation of goods to and from Newfoundland. This is an example of the many risk events that can impact the food supply network.

The aim of this joint project between Dalhousie University and the University of Strathclyde is to examine the resilience of food supply networks in Atlantic Canada using models to represent uncertainties and time effects in supply networks.

Our model examines resilience in an organization's non-perishable food supply network, which allows us to make inferences about the food supply to Newfoundland (see Figure 1). This network begins with suppliers located in the U.S. and Canada. Non-perishable goods are supplied to a centralized distribution centre (labelled A). They are then sent to North Sydney, Nova Scotia, where they are shipped via ferry to Channel-Port aux Basques, NL. From there the supply goes to a second centralized distribution centre (labelled B). The goods are then distributed to grocery stores throughout Newfoundland.

There are many risks that can affect the non-perishable food supply chain: storms might affect performance of marine transportation infrastructure; closure of the U.S./Canada border would impact supply; and inclement weather—such as strong winds—might impact ground transportation. Figure 2 shows the causal relationships between the variables in this event map.

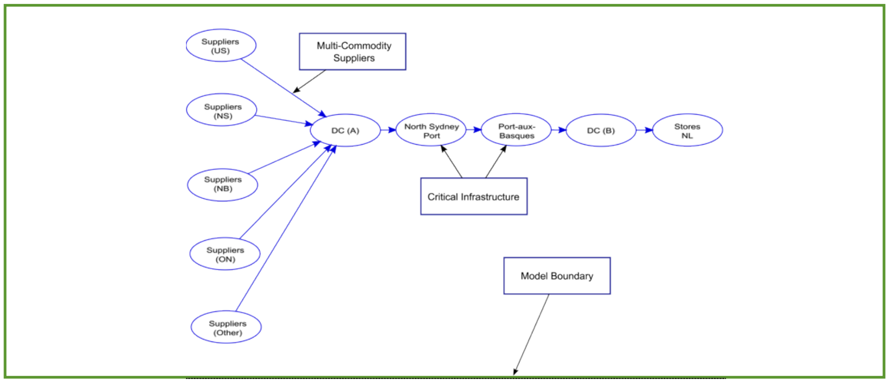


Figure 1: Non-Perishable Food Supply Chain

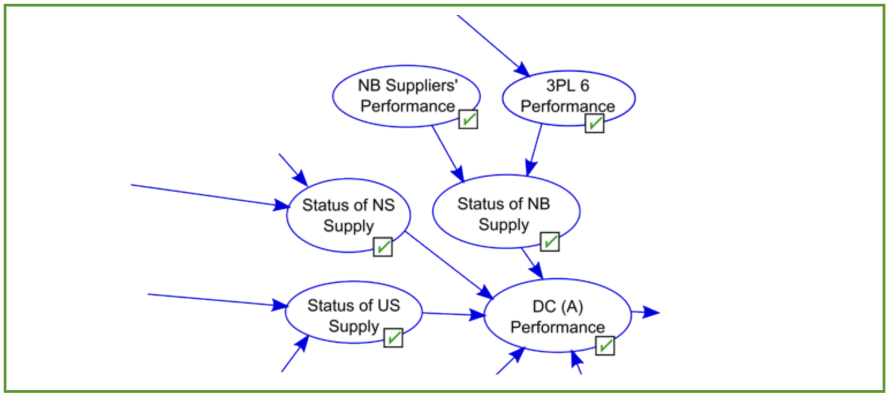


Figure 2: This section of the event map demonstrates the relationship between provincial supply chain performance and performance at distribution centre (DC) 'A'

To represent the time dynamics of the chain, we create a dynamic belief network (DBN) model (see Figure 3). This more formal model looks similar to a risk map; however, it differs because of the addition of feedback arrows on each oval to represent the time effects. Behind this visual model, the DBN model includes more formal statements to describe risk event 'states' and the probability they will occur given the impact of previous events. For example, a storm variable has two states:

TRUE - to represent the occurrence of a storm in a specific location within the considered time interval.

FALSE - to represent the non-occurrence of a storm in a specific location within the considered time interval.

These states are associated with probabilities to account for the uncertainty of their occurrence.

This study shows that distribution centre B, located in Newfoundland, is able to supply 92% to 95% of its orders about 60% of the time, despite the fact that ferries may only operate at about one-third capacity in the winter due to

Continued on page 12

Food supply network resilience in Atlantic Canada *continued*

disruptions. By carrying a high level of stock, the organization is able to maintain a high fulfilment rate despite fluctuations in reliability of ferry services. If we consider only the endpoint in the supply chain—the grocery stores—the network shows fairly stable performance during winter.

The organization's level of success is measured by its target fulfilment rate. For example, there is about a 60% chance that it will be able to fulfil 92-95% of its orders; however, there is a 20% chance that it will be below 92%. So, if the company's target fulfilment rate were 95% then it would miss the target 80% of the time, which means it would be successful only 20% of the time.

In addition to assessing supply chain performance during standard conditions, we considered what would happen if a hurricane were to pass through Newfoundland. Downstream members in the supply network, the Newfoundland distribution centre and ferry operators, are most likely to be impacted (see Figure 4).

The fulfilment rate would drop to and remain at 0% during the timeframe considered if no emergency measures had been implemented. We then examine a more reasonable scenario where mitigating actions are taken: governments implement emergency air shipments and take measures to restore infrastructure; the organization carries extra stock at the Newfoundland distribution centre, etc. Initially the fulfilment rate would drop to 0%, but after one week it would improve to 25%, due to the delivery of shipments via air. More time would be required for other emergency measures, such as recovery of marine transportation infrastructure, to take effect. The supply network would recover to its typical level of performance approximately 5 weeks following the hurricane.

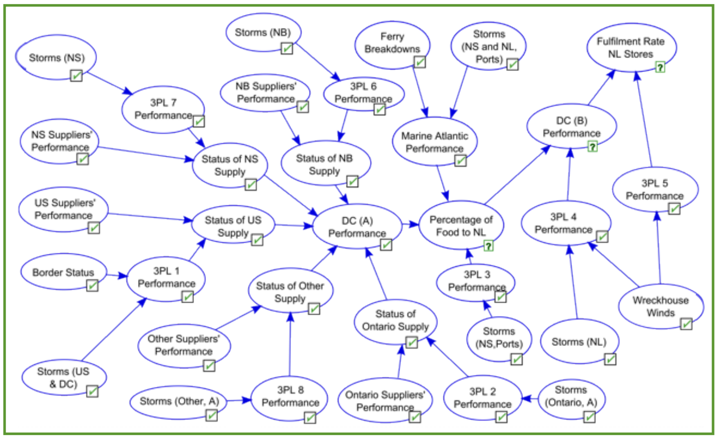


Figure 3: Dynamic Belief Model of Non-Perishable Food Supply Chain

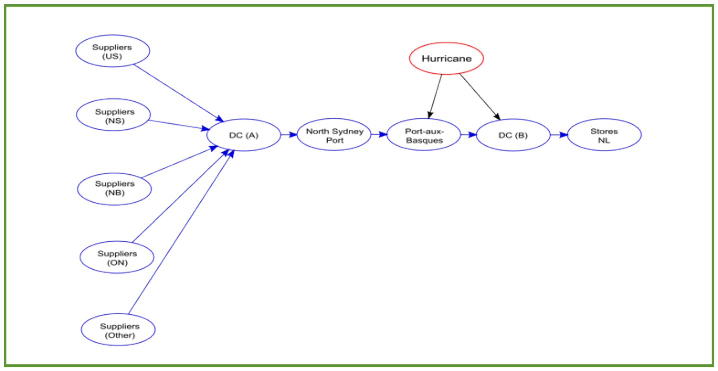


Figure 4: Scenario - Hurricane Hits Newfoundland

A hurricane is likely to impact grocery stores and regions differently. Newfoundland will be affected by loss of supply of non-perishable food products.
Based on our preliminary analysis, we find that government agencies have an important role to play in maintaining supply of non-perishable foods to Newfoundland after a hurricane.
As food supply is an issue of public interest, governments should implement measures to maintain the supply of non-perishable foods in Newfoundland in the event of a major risk event that could limit transportation infrastructure.

To conclude, the study demonstrates that modelling is an effective means of representing risk events and understanding how a supply network behaves both immediately after a catastrophic event and once emergency measures begin to take effect. The analysis presented above is based on simulated data; as such, results are only indicative of how the system may respond. The maps and models are informed by a real case study but have been altered in parts in order to keep the precise case maps and models confidential.

Mouhamad Ali Shaker Agha is a PhD candidate at the University of Strathclyde in Glasgow, UK, in the Department of Management Science. He is studying supply chain reliability and resilience modelling.
Email: ali.mouhamad-shaker@strath.ac.uk

The articles contained in this publication were prepared by their authors who are solely responsible for their correctness and appropriateness. The views contained in this publication are attributed to their authors and not to this publication, Dalhousie University or the Dalhousie School of Public Administration