Contract: No. 7181309 – "Identifying and Effectively Communicating Cyber-security Risks"

Communicating Effectively about Cyber-security Risks: Probabilities, Peer Networks and a Longer Term Education Program

Kevin Quigley**
Calvin Burns
Kristen Stallard

School of Public Administration
Dalhousie University

March 31, 2013

****Corresponding Author**
Kevin Quigley
kevin.quigley@dal.ca
School of Public Administration
Dalhousie University
6100 University Avenue
Halifax, Nova Scotia
B3H 4R2
902-494-3782

"It's 100% … OK. Fine. It's 95% 'cause I know certainty freaks you guys out. But it's a hundred." – CIA Intelligence Officer Maya commenting on the likelihood that Osama bin Laden is living in a compound in Abbottabad, *Zero Dark Thirty* (2012)

"It's a slam-dunk" – former CIA director George Tenet's now infamous reply to President Bush when he asked Tenet weeks before the U.S. invasion of Iraq whether or not U.S. forces would discover WMD in Iraq

Acknowledgments

The authors would like to acknowledge the support and contribution of Public Safety Canada towards this report.

Special thanks also go to the interview participants, Dr. Srinivas Sampalli of the Dalhousie University Faculty of Computer Science, and Dr. Lyn Bennett of the Dalhousie University English Department for sharing their time and expertise. We would also like to thank Janet Lord who copy edited this document.

Table of contents

1.0 About the authors

Kevin Quigley is an associate professor and director of the School of Public Administration at Dalhousie University. In 2008 he published *Responding to Crises in the Modern Infrastructure: Policy Lessons from Y2K* (Palgrave). Quigley specializes in public sector risk, strategic management and critical infrastructure protection. He has published in academic journals, such as *Public Administration, Health, Risk & Society, the Journal of Homeland Security and Emergency Management* and *Canadian Public Administration*. As principal investigator, he has secured over $800,000 in research grants and contribution agreements over the last six years in the area of risk, resilience and CIP. His recent projects include *Risk Governance in Theory and Practice: Connecting Canadian and UK Risk Networks to Improve the Resilience of Critical Infrastructure* (SSHRC Partnership Development Grant); *Critical Infrastructure Protection in Comparative Perspective: Contextual Factors that Influence the Exchange of Sensitive Information* (SSHRC Standard Operating Grant); *A Multi-Disciplinary Approach to Risk Governance: Best Practices, Workshops and On-line Training* (Innovative Public Management Research Fund, Canada School of Public Service) and *Critical Infrastructure Protection: Building Information-Sharing Networks across Sectors and Jurisdictions* (Innovative Public Management Research Fund, Canada School of Public Service). He is the editor of the professional publication *The CIP Exchange* and the co-founder of the *CIP Initiative* at Dalhousie University. Quigley has worked with government departments such as the Canada School of Public Service, Department of Foreign Affairs and International Trade, Defence Research and Development Canada, Public Safety Canada, Treasury Board Secretariat and New Brunswick Public Safety. Prior to starting graduate work, Kevin Quigley was a senior public servant in the Ontario Public Service. Among other responsibilities, he was Project Lead on Walkerton at Cabinet Office Communications.

Co-Principal Investigator: Calvin Burns is lecturer in organizational psychology at the University of Strathclyde Business School, Glasgow, UK. He conducts research mainly in high-hazard organizations like hospitals, oil companies, and construction firms. His research interests in these organizations include Trust, Safety Culture / Climate, Risk Perception and Communication, and Implicit Cognition. Calvin has worked extensively with Kevin Quigley on many funded projects (as described in Kevin's resume above) and has published recently in *Risk Analysis* and the *Journal of Risk Research.*

Kristen Stallard (MPA Candidate 2013) is in the second and final year of the Dalhousie University Master of Public Administration program. She holds a Bachelor of Arts (Honours) in Political Science from St. Francis Xavier University and a Master of Arts in Political Science from the University of Toronto. In 2010, Kristen was the recipient of a Joseph-Armand Bombardier CGS Master's Scholarship from the Social Sciences and Humanities Research Council of Canada. Her research interest is in Canadian municipal government.

2.0 Executive summary

Context

This report was commissioned by Public Safety Canada in 2012. The goal of the project was to conduct a rhetorical analysis of how 'management gurus' communicate in newspapers, popular books, and online fora about cyber-security. Management gurus can be described as the consultants, academics, and authors who profit from selling solutions to complex organizational issues like cyber-security. The study of modern management guru techniques was initiated by Huczynski in 1993. Following our rhetorical analysis, we interviewed a small sample of public managers with responsibility for IT; we sought to determine whether or not the management gurus' narratives aligned with the manner in which public sector IT managers think about cyber-security. Based on this research, we recommend institutional practices and policies that government agencies can adopt to support more effective communication about cyber-security.

This is a brief study conducted during a short time frame. As such, there are important methodological constraints to acknowledge. First, due to the limited time available, we were only able to interview a small number of subjects. In order to ensure that our findings from this small sample would be representative, we only interviewed *public sector* managers. They were sampled from different regions and different public sector organizations and the interviews were designed to be inductive and exploratory. Despite these limitations, common themes emerged from the interviews, which were reinforced by our literature review and aspects of our rhetorical analysis. Based on this, we make some recommendations but also call for further research on the themes we discuss here. We outline a future research agenda at the end of the executive summary and in the conclusion.

Literature Review

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 within the supply chain. There are notable discrepancies in other areas of the literature, however, such as how people construct their perceptions of risk and whether these perceptions are shared by technical experts and laypeople. This report draws on the literature as well as a rhetorical analysis and qualitative interviews to fill some of these gaps.

The literature review of the report highlights that:

- The psychology literature suggests that risk perceptions are subject to biases.
- The management guru literature is shown to be a useful way to understand how cyber-security risks are emphasized and often exaggerated in popular media.
- The cyber-security literature argues that cyber-crime and 'hacktivism' are the most serious threats; nonetheless, cyber-terrorism and cyber warfare receive the most attention.
- The availability heuristic and common management guru techniques are found to be at play in the discussion of risks supposedly posed by cyber-terrorism and cyber-warfare.

Rhetorical Analysis

A rhetorical analysis conducted on ten samples – including articles written by politicians, public servants, journalists, CEOs, academics, and computer scientists – finds evidence that:

- The samples rely on rhetorical devices and heuristics to convince the reader about the risks supposedly posed by cyber-security.
- The samples are convincing in their discussion about the vulnerabilities in our daily lives to cyber-crime and 'hacktivism.'

- The samples are not convincing in articulating the risks posed by cyber terrorism and cyber warfare.
- The literature largely focusses on worst case scenarios and overlooks or supresses information about probabilities.

Findings from interviews

Qualitative findings from interviews conducted with public sector cyber-security practitioners in Canada and the United Kingdom uncover:

- People working in different public sector contexts understand cyber-security differently. Across these contexts, three themes emerged: 1) protection of privacy, 2) protection/integrity of information, and 3) protection of systems/assets.
- Cyber technology offers flexibility and innovation in service delivery but introduces risks to information security, especially from information kept on mobile devices. When considering these risks, decision-makers are aware of both the likelihood and consequences of a cyber-security breach.
- The media plays a role in bringing some issues / trends about cyber-security to people's attention but decision-makers in public sector organisations tend to be influenced most by peer networks.
- Interview subjects seemed more concerned about data privacy and integrity and less concerned about terrorism, sabotage and/or vandalism.

Conclusions

The Internet and related information technologies pose common challenges that few people actually understand. There is not at present a consensus on the best way to address the risks associated with cyber and cyber-security. There are, however, common concepts that are integral to discussions about receiving advice about cyber-security, including confidentiality, integrity and credibility. As demonstrated by our analysis, the ambiguity about how best to proceed in cyber-security has left policy-makers, the media, and the public vulnerable to exploitation by cyber-security gurus who could potentially manipulate laypeople into believing that threats posed by information technology are imminent and dire, even without offering sound evidence to justify such a claim. Despite this burgeoning management guru theme, it is not clear that IT public sector managers are convinced by the claims of management gurus at present. Generally, IT managers are motivated by the potential for IT innovation. They express concerns about risks associated with, for example, data integrity, intellectual property, privacy, reputation and the trustworthiness of security information.

Recommendations

IT public sector managers belong to peer-networks within public services; these networks are based on trusting interpersonal relationships. Public sector organizations should recognize the importance of these peer-networks for managing cyber-security risks and develop and support them.

Institutional arrangements should reinforce the importance of cyber-security. The interviews revealed that some IT managers thought that cyber-security was a shared responsibility between IT and the people who are using the organization's IT systems and information. While sharing responsibility for critical resources is laudable, public agencies must

actively promote responsible IT security behaviours among the staff and clarify roles and responsibilities lest the ambiguity over responsibility become an opportunity for blame-shifting between parties when things go wrong. Each public organization should also have a highly visible and accessible "cyber-security champion" who promotes awareness of cyber-security issues. This appointment will not only bring attention and resources to the subject, but will also provide a reliable internal resource that can offset the potentially powerful influence of external IT consultants whose incentives are not necessarily aligned with the public organization's goals.

Governments should be more specific about the terms they use to describe breaches in cyber-security. We discuss four types in this paper: cyber-crime, 'hacktivism,' cyber-terrorism, and cyber-warfare. The perpetrators of each are driven by different motives and the solutions to each will also be different. Equally, public officials should be mindful of the metaphors they employ. Our research suggests that the metaphor of cyber as a 'battlefield,' for example, is overused and is often inaccurate. The metaphor implies that the risk should be understood in terms of survival as opposed to a trade-off between costs and benefits; this distinction has a potentially powerful impact on the manner in which one approaches a risk problem.

Indeed, government officials must develop a more nuanced understanding of risk. Our comments here are constrained somewhat due to the fact that reliable information related to cyber-warfare and cyber-terrorism is not easily available. Neither industry nor government readily disclose such information (Quigley 2013). That noted, the rhetorical analysis section demonstrates that management consultants emphasize extreme consequences and either overlook, suppress or exaggerate probabilities depending on the point the consultants wish to make. When, for instance, should government strategies and operations be guided by 'worst case scenario' thinking? Precautionary approaches to managing risks are expensive (Sunstein, 2005).

Taking a precautionary approach with a specific risk includes a price in terms of opportunity cost, and inevitably increases other (often less visible) risks, intentionally or unintentionally. What is the potential opportunity cost of not having progressive social media policies that allow public servants to engage with the citizenry in online fora, for instance? Government must develop a more effective method to prioritize systems and the security required for such systems. Sunstein (2009) advises that we should consider catastrophic and irreversible harms – particularly to human and environmental safety – as the risks that require a more cautious approach and have a more balanced approach with the others. Interview subjects reinforced this observation.

Relatedly, we may be at a point where the very notion of privacy must be reconsidered. Interview subjects noted that certain information is protected but it need not be, or at least not to the standard to which it presently is: people's expectations about what should be private are changing. There are potentially significant resource and democratic implications to keeping information private. We need to have a better understanding of what really needs to be protected to a high level and what does not. Public bureaucracies are susceptible to regulating in the face of uncertainty; over-regulating information availability jeopardizes the potential innovation and transparency of public institutions.

Government must acquaint itself with an industry perspective in order to communicate more effectively with industry. Government interests and practices at times differ from those of industry. As one interview subject noted, strategists for national defense, for instance, often interpret risks in terms of its capacity to withstand an attack from an enemy. In this calculation, survival is always paramount. When the survival of an organization is at stake, risk can no longer be described as the product of probability and expected monetary losses. In the case of national

defense, there is at times a disproportionate focus on consequence with relatively less focus on probability. In contrast, industry balances dangers with financial opportunities. Industry is not necessarily interested in international espionage or cyber-warfare; it is often more interested in insider threats, extortion, industrial espionage, intellectual property, the protection of financial data and learning best practices from others in its sector. To assist industry, government can help to facilitate the exchange of information and establishment of standards in these areas in particular.

Government must also understand the needs of the public. Consumers of government services expect to be able to use a variety of mobile devices to find information specific to their needs (Flumian, 2009). Politicians often support these initiatives on behalf of their constituents and moreover, would like to engage with their constituents on one of a number of devices and on one of a number of social media sites. Mobile devices and the fusion of data represent increased opportunities and risks. While there may be some exceptions, such as identity theft, the research we conducted suggests that the public is not particularly concerned about many aspects of cyber-security. Meeting this demand for flexibility—from the public and the elected officials—will continue to exert pressure on public officials with responsibility for cyber-security.

Most cyber events lack the characteristics of a 'good' media story (e.g., 'catching a bad guy') and therefore tend not to be included in popular media coverage (Fowler and Quigley, nd). Lately, we have seen a rise in coverage of cyber bullying. Child abuse – whether cyber or not – generates considerable media coverage and it can often be highly emotionally charged (Hood, Rothstein and Baldwin, 2001; Fowler and Quigley, nd). The government needs to use these types of events to raise awareness, not in an anxiety-generating way but rather to encourage a more sophisticated understanding of risks associated with the Internet in a manner in which people can

identify in their personal lives. Some have argued that cyber-security is a civic duty (Harknett and Stever, 2009) though to date this argument has failed to take hold. More education in schools and at home about cyber risks will enhance our understanding of the issues. In turn, this focus will allow people to better protect themselves and also contribute to policy discussions about what level of risk we are prepared to tolerate in cyber-space, and how active the government should be in this policy area. While an education program is crucial, it must take a longer-term view.

Recommended next steps for this research

As noted, the interview study was based on a small sample of public sector managers. We recommend conducting a larger-scale interview study with participants from both the public and private sectors. This would allow for comparison of how public and private sector managers monitor the external environment for emerging cyber-security threats and opportunities, and a comparison of best practices between the sectors. It would also be useful to compare how owners and operators of large critical infrastructure entities such as healthcare and power supply perceive cyber risks to small and medium-sized operators, such as those found in the manufacturing and agricultural sectors.

Finally, we believe it is also important to explore issues of diversity. White males, non-white males, and women typically receive, process, and act on risk messages differently (see, for example, Finucane et al., 2000; Flynn et al., 1994). As email, texting and social media become the communication tools of choice, we believe it is crucial to explore how this affects online behavior and perceptions of risk.

3.0 Introduction

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 (Kolluru and Meredith, 2001; Faisal et al., 2006). 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. There is also an implicit assumption that IT knowledge and risk perceptions are shared equally between technical experts and lay persons. This project seeks to address some of these gaps in the existing cyber-security literature.

There are three purposes to this paper. The first goal is to provide an understanding of the context in which cyber-risk is constructed. Special focus will be paid to how people make (often erroneous) judgments about risk. Afterwards, the literature on so-called "management gurus" will be examined. This literature refers to the industry of consultants, academics, and authors who profit from selling solutions to complex organizational issues like cyber-security. Next, the ways in which contemporary cyber-security issues are framed in the literature will be broadly explored. This information will then be used in a rhetorical analysis to determine whether management gurus are using traditional guru techniques to over-dramatize or over-simplify cyber-security problems for their benefit.

The second purpose is to present the findings from interviews with decision makers from public sector organizations about cyber-security. Given people's limited capacity to process risk information and the potentially persuasive manner in which cyber gurus are describing the cyber threat, we are particularly interested in gauging how public sector managers with responsibility for IT understand the risks associated with the Internet and the actions they take to protect their

systems. In other words, we would like to know if the cyber gurus are having an impact on the manner in which public sector IT managers understand IT risk.

Finally, in the conclusion, we summarize our key findings and provide recommendations about how, at the institutional level, Public Safety Canada might address some of the risks associated with potentially exaggerated claims about cyber-security. The ultimate goal will be to question the effectiveness of how we talk about and raise awareness of cyber-security issues in general.

The paper is organized in the following manner. First, we summarize the psychology-of-risk literature, the management guru literature, and trends in the critical cyber-security literature. Secondly, we include a rhetorical analysis of ten samples drawn from diverse sources, including politicians, public servants, journalists, CEOs, academics, and computer scientists, all commenting on the subject of cyber-security. Thirdly, we report the findings from our interviews about cyber-security with decision makers from public sector organizations. Finally, we summarize our findings and include recommendations for Public Safety Canada about how, at an institutional level, government can help to improve social discourse about cyber-security.

4.0 Literature review: Bridging divergent perspectives to understand cyber risk

Section summary

- The psychology literature suggests that risk perceptions are often faulty.
- The management guru literature is shown to be a useful way to understand how cyber-security risks are exaggerated in popular media.
- The cyber-security literature argues that cyber-crime and 'hacktivism' are the most serious threats; nonetheless, cyber-terrorism and cyber warfare receive the most attention.
- The availability heuristic and common management guru techniques are found to be at play in the discussion of risks supposedly posed by cyber-terrorism and cyber-warfare.

This literature review draws on three sources of research: the psychology-of-risk, the literature on management gurus, and the literature on cyber-security. Taken together, they demonstrate how people construct risk perceptions as well as how these perceptions can be thrown off-course by persuasive management gurus. This information is used in the next section to analyze the specific dangers posed by cyber-security as part of a rhetorical analysis.

4.1 The psychology of risk

Risk cannot be directly observed. Rather, it is constructed by people based on their understanding of hazards in everyday life. According to Burns (2012), it is important to understand risk for two reasons. Firstly, risk perception helps us to understand and predict people's behavior. Secondly, awareness of how perceptions are constructed helps to improve communication between technical experts and laypersons.

Generally speaking, there are two types of risk: risk as analysis and risk as feelings (Slovic and Peters, 2005). Risk as analysis uses logic, reason, and scientific deliberation to assess hazards. These types of hazards are measurable using statistical evidence or theoretical models. By contrast, risk as feelings is related to our intuitive or emotional response to hazards. These types of hazards are subjective and derived from beliefs, attitudes, or judgments. According to Slovic and Peters (2005), intuitive perception of risk is the dominant method by which people

assess threats. The question is whether these perceptions accurately reflect the magnitude, frequency, and probability of actual hazards.

A central finding of the psychology literature is that perceptions are often, in fact, faulty. People typically make judgments about risk using incomplete or erroneous information. They also rely on judgmental biases or heuristics to comprehend complexity. Heuristics are cognitive tools that influence how people perceive risk (Slovic et al., 1982). In some ways, heuristics are helpful; they allow people to render simplistic understandings of complicated subjects. However, they can also oversimplify or distort our understanding of complicated subjects.

Slovic et al. (1982) note that heuristics fall along two primary dimensions: the unknown factor and the dread factor. The unknown factor influences people to be less concerned with risks that are "observable, known to the exposed, have immediate effects, and are known to science" (Slovic et al., 1982, p. 86). On the other dimension, the dread factor influences people to be less concerned with risks that are "controllable, not dreadful, not globally or individually catastrophic, equitable, pose low risks to future generations, are easy to reduce exposure to, are voluntary, and are overall decreasing" (Slovic et al., 1982, p. 86). These two dimensions indicate just how far risk perceptions can go off track.

Slovic et al. (1979) have compiled some of the most common heuristics in risk perception: availability, overconfidence, and desire for certainty. These biases frequently misconstrue the true nature of risk. As a result of these faulty perceptions, efforts to manage risk can therefore be made in vain, wasting valuable time, effort, and resources in the process.

Availability

Using the availability heuristic, people will believe that an event is more likely to occur if they are able to imagine or recall it (Slovic et al., 1979). For example, the authors note that fear

of shark attacks increased dramatically after the release of the movie *Jaws*, despite the fact that there was no empirical evidence to suggest that shark attacks had become more probable (Slovic et al., 1979).

By contrast, availability can also lull people into a false sense of security regarding the risks associated with everyday tasks (Slovic et al., 1979). Few people consider the risks associated with starting their car, for example. As these two examples suggest, risks that are overestimated are typically dramatic and rare with the availability heuristic. By contrast, underestimated risks have a much more subdued impact and are much more commonplace (Slovic et al., 1979).

Overconfidence

Using the overconfidence heuristic, people tend to be convinced that their risk perceptions are accurate. This bias occurs even in the absence of evidence to support overconfident assumptions. Slovic et al. (1979) suggest that the overconfidence heuristic is based on our insensitivity to how little we actually know or understand. This heuristic can be particularly troubling for experts. Slovic et al. (1979) note that experts are prone to overlook the influence of human error, miscalculate human responses to safety measures, and assume that current scientific knowledge is accurate and complete. In other words, the overconfidence heuristic can lead people to overestimate their personal safety or underestimate threats.

Desire for certainty

Finally, psychologists have found that people try to overcome their anxieties by relying on the third heuristic, the desire for certainty. Uncertainty is inherent in life; however, people often fail to acknowledge it or ignore it altogether. Instead, they either display complete denial or require complete certainty when neither is possible to guarantee. The desire for certainty

heuristic occurs in the approval of new foods or drugs, for example. Slovic et al. (1979) recall an instance in which scientists were only able to offer a 95 per cent probability that artificial sweeteners did not cause cancer. Consequently, their stance was criticized by U.S. Food and Drug Administration policy-makers who were trying to ascertain the safety of artificial sweeteners for human consumption. The desire for certainty heuristic can therefore lead people to jump to conclusions about the likelihood of risk or deny its existence altogether if they feel unable to control it.

As these three examples indicate, heuristics are extremely influential cognitive tools. They are frequently used to understand complex subjects. However, heuristics can also skew risk perceptions. Furthermore, as research conducted by Slovic et al. (1979) indicates, beliefs based on heuristics are also "slow to change and extraordinarily persistent in the face of contrary evidence" (p. 37).

> New evidence appears reliable and informative if it is consistent with one's initial beliefs; contrary evidence tends to be dismissed as unreliable, erroneous, or unrepresentative. When people lack strong prior opinions, the opposite situation exists – they are at the mercy of the problem formulation. Presenting the same information about risk in different ways buffets their perspectives and their actions like a ship in a storm (Slovic et al., 1982, p. 85).

Therefore, understanding how risk perceptions are formed is critical to making informed judgments about how to manage risk. Of the three heuristics profiled here, availability is considered to be the most important for understanding risk perception (Sjöberg, 2000). Media attention is often a key factor, elevating the public's perception of risk through frequent exposure.

The study of risk perception began in the 1960s when fears about nuclear warfare were at their peak (Sjöberg, 2000). Notably for this project, terrorism has since replaced nuclear warfare as today's most widely dreaded risk (Slovic and Peters, 2005). This trend continues despite the

fact that both nuclear warfare and terrorism are considered to be extremely unlikely to occur. In psychology, this phenomenon is referred to as 'probability neglect' or insensitivity to the probability of an event.

Probability neglect is often accentuated by an emotional reaction to extreme events. In the case of terrorism, for example, ''probability neglect is highly likely in the aftermath of terrorism. … When probability neglect is at work, people's attention is focused on the bad outcome itself, and they are inattentive to the fact that it is unlikely to occur" (Sunstein, 2003, p. 122). Nevertheless, fears about terrorism have grown dramatically since the September 11, 2001, terrorist attacks and continue to influence the way in which people perceive all threats. This context helps to explain the literature on management gurus profiled next.

As this section indicates, perception is particularly important for risk management, especially at the phase of designing solutions to prevent or mitigate risk. If perceptions are wrong, they can have a disastrous impact on efforts to manage risk. Erroneous perceptions can produce dire consequences for supply chains, the environment, and the public (Slovic et al., 1979). As such, psychologists have built an extensive body of literature related to how risk is perceived and assessed by humans. The benefit of this research – and its relation to this project – is that it raises awareness about heuristics and can therefore help to reduce their negative influence on risk perceptions.

This valuable information can be used in a variety of ways. First, it helps researchers to anticipate which hazards will concern people. Secondly, it can be used to find ways to lessen misplaced fears. These findings about risk perception help to next explain the persuasive power of management gurus.

4.2 Management gurus

The term ‘management guru’ refers to the proponents of popular management thought and practice. It includes the authors, publishers, editors, consultants, managers, commercial seminar organizers, and professors who offer advice on business and management (Kieser, 1997). The study of organizational structures began at the beginning of the 20th century and accelerated after World War II. It spread through the proliferation of specialized business schools, the creation of MBA programs, and the publishing of influential management books (Huczynski, 2006). Popular themes of this industry have traditionally been organizational behavior, change management, and innovation.

One of the watershed moments in the management guru movement was the publishing of Peters and Waterman’s best-selling book *In Search of Excellence* in 1982. The success of Peters and Waterman inspired Andrzej Huczynski to write the first historical analysis of the management guru phenomenon in 1993. Huczynski was primarily interested in why management ideas were so popular, particularly among managers. Furthermore, he questioned why, given their popularity, leading management ideas of the day were rarely taught in academia (Huczynski, 2006).

A new academic field emerged from Huczynski’s initial study. This new field has been interested in “how management knowledge is created, processed into saleable products and services, how it is marketed, communicated to customers, and how it is consumed by them” (Huczynski, 2006, p. 2). The field has also attracted business and management academics critical of the ambitious prescriptions offered by management gurus. The management guru literature can therefore be understood as both a reaction against and response to the popular literature on business and management.

As the literature notes, management gurus are considered to be influential because they inspire managers to implement their solutions to solve complex organizational problems (Huczynski, 2006). A key finding of the literature is that these cures come and go over time. Kieser (1997) likens the rise and fall of management trends to the fashion industry. He notes that, "at the start of the fashion, only a few pioneers are daring enough to take it up. These few are joined by a rising number of imitators until the fashion is 'out' and new fashions come on the market" (Kieser, 1997, p. 51). In addition to explaining the rise and fall of management trends, this metaphor is helpful for capturing the influential role that aesthetics play in management trends as well.

Røvik (2011) argues that the rise and fall of management trends can also be compared to the lifecycle of a virus. The virus theory helps to explain what happens to organizations once they have been 'infected' with a new organizational idea. Organizations typically go through the stages of "infectiousness, immunity, replication, incubation, mutation, and dormancy" before the next fad takes hold (Røvik, 2011, p. 635). Interestingly, organizations do not build immunity to management fads over time. Despite the fact that guru ideas have only a modest impact on actual working life, managers always seem prepared to entertain the next trend.

One of the central questions of the literature is why managers are particularly susceptible to guru ideas, especially given their limited practical results. Ahonen and Kallio (2009) argue that guru ideas are a form of cultural expression. From this perspective, the management model is the Holy Grail "to which all seemingly good values and ideas have been projected" (Ahonen and Kallio, 2009). Much like the quest for the Holy Grail, the search for the ideal management model is more important than the model itself. It also represents many ideals in liberal Western democracy, such as the never-ending quest for "efficiency, success, and welfare" (Ahonen and

Kallio, 2009, p. 433). As such, the search for the best management ideas can be considered to serve a therapeutic role for both managers and gurus alike.

Other researchers explain the appeal of gurus through their impressive performances. Clark and Salaman (1996) liken these performances to that of a witchdoctor since gurus give "a 'dramatic realization' in which the performer conveys to an audience that which they wish to express" (p. 91). In a later study, Clark and Salaman (1998) add that management gurus help to construct the identity of senior managers as heroic and transformative leaders. This depiction is at odds with the traditional view of managers as the victims of rhetoric used by gurus. Werr and Styhre (2003) find support for this argument in a study of business leaders in Sweden, discovering that managers assert their control and superiority over consultants in order to defend their identity as managers.

The management guru literature also accounts for how popular management ideas become influential. One of the fundamental findings of the literature is that rhetoric is the most common and influential management guru technique. For example, Hood and Jackson (1991) argue that persuasion fuels organizational change more often than objective facts. In their view, management gurus attempt to establish their theories as the most credible, not necessarily the most truthful (Hood and Jackson, 1991). To this end, Hood and Jackson (1991) identify six salient features of guru theories: their universal appeal, contradictory nature, instability, use of recycled ideas, reliance on soft data and logic, and competition with rival ideas through aesthetics rather than evidence.

Berglund and Werr (2000) support Hood and Jackson's (1991) typology, adding that management gurus rely on the use of contradictory business myths or ideas to adapt their arguments to suit any need or audience. Furthermore, Keulen and Kroeze (2012) bring attention

to the way in which management gurus frame their arguments using historical narratives or anecdotes to express the soundness of their ideas. The use of anecdotes is also a persuasive method to position management gurus as the purveyors of practical knowledge in direct contrast to the theoretical knowledge offered by academics. This positioning lends management gurus affinity with managers as 'one of us' (Huczynski, 2006).

It is worth noting that the public sector is not immune to this trend either. The public sector was most famously captured by the 'reinventing government' movement, which rested on the assumption that governments and the public sector should learn from the private sector (Osborne and Gaebler, 1993; also see Moore, 1995, *Creating Public Value*; see also Osborne, 1998, *Banishing Bureaucracy*). Much like traditional management guru ideas, the use of highly rhetorical arguments characterized the 'reinventing government' movement as well.

As this section illustrates, management gurus are the persuasive purveyors of popular ideas in administration, business, and management. They capitalize on the aspirations of managers in order to sell their ideas. As shown in the critical literature, management gurus owe much of their success to the rhetorical techniques they employ rather than to the soundness of their arguments. They rely on factors like aesthetic appeal and soft logic to convince managers to adopt their solutions. Despite the limited practical impact of management guru ideas, they nonetheless continue to be popular among managers as they search for the next solution to remedy complex organizational challenges.

Management guru literature is connected to this project by the way gurus are able to overdramatize or oversimplify complex organizational issues for their benefit. As will be demonstrated in the next section, there is a similar pattern occurring in the literature on cyber-

security. Indeed, management guru strategies are a useful way to understand how cyber-security risks are exaggerated in popular media.

4.3 Trends in the cyber-security literature

In the early 1990s, computer scientists used 'cyber-security' as a technical term to describe insecurities in networked computers. Soon after, however, this term was co-opted by elected officials, the media, and the private sector, particularly in the United States. Phrases such as 'electronic Pearl Harbors' and 'electronic weapons of mass disruption' began to be used to characterize the threats supposedly posed by the Internet and other forms of information technology (Hansen and Nissenbaum, 2009). This section details the critical literature on cyber-security, focusing on flaws in the framing of threats and the ways in which they have been exploited to justify expensive countermeasures.

Cyber-security first coalesced into a threat in U.S. national security literature after the Cold War. As early as 1991, technology was said to enable enemies of the United States "to do more damage with a keyboard than with a bomb" (Cavelty, 2007). Thus, early cyber-security literature invoked Cold War fears like nuclear war to depict threats supposedly posed by technology. This framing evolved following the 1995 Oklahoma City bombing. Based on this high-profile incident, cyber-security began to be closely linked with terrorism and critical infrastructure vulnerabilities (Cavelty, 2007). The connection was solidified following the September 11, 2001, terrorist attacks in New York City, Pennsylvania, and Washington, DC. Phenomena such as the Y2K sensation and the creation of the Internet also play into fears about the capacity of technology to create havoc as well as threaten bureaucratic power (Stohl, 2006; Quigley 2008).

Today, there are four main depictions of threats in the cyber-security literature: cyber-terrorism, 'hacktivism', cyber-crime, and cyber warfare. Cyber-terrorism is by far the most popular topic. Terrorism is commonly defined as "the purposeful act or the threat of the act of violence to create fear and/or compliant behavior in a victim and/or audience of the act or threat" (Stohl, 2006, p. 229). Cyber-terrorism means that these acts are committed using technology. 'Hacktivism,' meanwhile, refers to "the marriage of hacking with political activism" (Stohl, 2006, p. 236). Cyber-crime refers to criminal offenses committed online or through other forms of IT. Finally, cyber warfare refers to "the role of information technology as an enabler of warfare" (Colarik and Janczewski, 2012, pg.39).

Combined with technology, cyber-terrorism is said to achieve two objectives: effects-based or intent-based terrorism:

- *Effects-based:* Exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals;
- *Intent-based:* Exists when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage (Stohl, 2006).

However, authors such as Lewis (2003), Stohl (2006), Cavelty (2007), and Hansen and Nissenbaum (2009) all note the lack of empirical evidence to support the widespread fear of cyber-terrorism. According to Cavelty (2007):

> While governments and the media repeatedly distribute information about cyber threats, real cyber-attacks resulting in deaths and injuries remain largely the stuff of Hollywood movies or conspiracy theory. In fact, menacing scenarios of major disruptive occurrences in the cyber-domain, triggered by malicious actors, have remained just that – scenarios. Nonetheless, for the US government (and to a lesser degree other governments around the world), the decision has been far more straightforward: it considers the threat to national security to be real, has extensively studied various aspects of cyber-threats, and spends considerable sums on a variety of countermeasures (p. 20).

In fact, Stohl (2006) notes that there is little vulnerability in critical infrastructure that could even lead to violence or fatalities. Secondly, there are few actors who would be interested in or capable of exploiting such vulnerabilities. Thirdly, the expenses necessary to carry out cyber-attacks are greater than traditional forms of terrorism, limiting the utility of cyber-attacks compared to other available measures (Stohl, 2006). Instead, technology is most often used by terrorists to provide information, solicit financial support, network with like-minded terrorists, recruit, and gather information – in other words, "terrorist groups are simply exploiting modern tools to accomplish the same goals they sought in the past" (Stohl, 2006, p. 230). Despite the lack of evidence, however, the literature on cyber-security threats from cyber-terrorism continues to grow.

In reality, cyber-terrorism is often mistaken for other, more commonplace cyber-security threats. 'Hacktivism' is one major issue highlighted in the cyber-security literature. This term describes computer hackers who disrupt or manipulate vulnerabilities in computer systems or software for the purposes of political activism. Typically, hackers use "virtual sit-ins and blockades; automated e-mail bombs; web hacks and computer break-ins; and computer viruses and worms" to draw attention to their cause (Stohl, 2006, p. 236). While 'hacktivism' does encompass the political aspect necessary to categorize these kinds of attacks as cyber-terrorism, the objective of hackers is more often to cause mischief for the targeted organization than to cause violence or deaths. Cyber-crime is also a major issue noted in the cyber-security literature, but it is more problematic for law enforcement and businesses (Lewis, 2003). The most common forms of cyber-crime include "insider threats, extortion, industrial espionage, and loss of financial data or intellectual property to outsiders" (Lewis, 2003).

Despite their relative frequency, threats from 'hacktivism' or cyber-crime are frequently overshadowed by the fear of cyber-terrorism in the popular press. As a result, they often fail to be noticed or are misrepresented as acts of cyber-terrorism. Ironically, this error has the effect of increasing the popular fear of cyber-terrorism while more common forms of cyber-security risk like 'hacktivism' or cyber-crime remain largely ignored.

As this discussion of the cyber-security literature suggests, technology is now conceptualized as more than a tool by the general public; it also has the potential to be wielded as a weapon. Hansen and Nissenbaum (2009) explain how technology has been transformed into a distinct security threat using the Copenhagen School's theory of securitization. The Copenhagen School positions the security industry as a unique discourse with its own rhetorical structure and political effects. From this perspective, security is a "speech act that securitizes, that constitutes one or more referent objects, historically the nation or the state, as threatened to their physical or ideational survival and therefore in urgent need of protection" (Hansen and Nissenbaum, 2009, p. 1156). Interestingly, when first proposed in the 1980s, the theory of securitization excluded threats emanating from technology. The justification at the time was that cyber-security threats did not influence the framing of other security issues. Today, by contrast, technology is considered to be the "common underlying factor upon which all security sectors are destined to converge" (Yould, 2003, p. 78).

Cyber-security is captured by the theory of securitization in three distinct ways:

1) Hyper-securitization, which identifies large-scale, instantaneous, cascading disaster scenarios;
2) Everyday security practices that draw upon and securitize the lived experience a citizenry may have; and
3) 'Technifications,' that captures the constitution of an issue as reliant upon expert, technical knowledge for its resolution and hence as politically neutral or unquestionably normatively desirable (Hansen and Nissenbaum, 2009, p. 1157).

From this perspective, casting cyber-security threats as a security issue – instead of a purely political, economic, criminal, or technological problem – has distinct ramifications. First, this perspective is powerful because it requires a multi-disciplinary lens to understand. Cyber-security involves political, economic, criminal, and technological dimensions all at once. Secondly, the 'technification' aspect means that experts acquire a more privileged position in the discourse, making it harder to challenge prevailing norms. Finally, the hyper-securitization of everyday technology brings the fear of technology to the forefront of the popular media. In other words, the public has become ultra-sensitive to the threats supposedly posed by technology, leaving them vulnerable to the persuasion of cyber-security management gurus.

This section has outlined some of the main themes in the cyber-security literature. It has shown how cyber-security has evolved from a technical term used almost exclusively by computer scientists in the early 1990s to a potential 'weapon of mass destruction' in the post-9/11 era. This section also describes the most common cyber-security threats – like 'hacktivism,' and cyber-crime – and illustrates how cyber-terrorism overshadows them all in the popular media. Most importantly for this project, the information gathered from the cyber-security literature highlights common heuristics and management guru techniques that are being used in the cyber-security field.

The most obvious heuristic at play is availability. As earlier sections note, the availability heuristic influences people to believe an event is more likely to occur if they are able to easily imagine or recall it. In terms of cyber-security, fear of technology intensified following high-profile incidents like the Oklahoma City bombing, Y2K, and the September 11, 2001, terrorist attacks. The media played an important role in propagating the fear of technology at the time, giving these incidents extensive exposure and searing them into popular culture. Finally, the

emotional response invoked by these traumatic incidents has made the public more sensitive to these types of incidents, even when they are considered to be very unlikely. As the psychology literature predicts, the availability heuristic has therefore influenced policy-makers, the media, and the public to be fearful of similar attacks – most notably in the form of cyber-terrorism – even when there is little to no empirical evidence to support such a fear.

In terms of management guru techniques, there are four prominent techniques at play. Firstly is the use of historical narratives. Cyber-security management gurus have conveyed the severity of threats posed by information technology by making reference to Pearl Harbor, the Cold War, and the War on Terror. These associations influence the public to relate cyber-security issues to these major events. Secondly, framing cyber-security as a combined political, economic, criminal, and technological problem recalls the guru technique of using contradictory discourses to change an argument to suit any need or audience. Thirdly, the importance of technical experts in this field also makes it difficult to challenge gurus or their claims. Fourthly, positioning cyber-security as a terrorist threat recalls the cultural role that management gurus play. Much like the War on Terror, the quest for cyber-security solutions is never-ending. Therefore, the search for a solution to cyber-security threats – and cyber-terrorism in particular – serves a therapeutic role for the public as it lives in constant fear of future attacks.

As these examples suggest, heuristics and management guru techniques are powerful tools. Furthermore, they are prevalent in the cyber-security discourse and are being used to exaggerate threats supposedly posed by information technology. The next section will provide additional evidence to support this argument by performing a rhetorical analysis on several samples from the cyber-security discourse.

5.0 Rhetorical analysis: Cyber-security discourse examined

Section summary

- Rhetoric involves stylistic devices and various types of arguments to develop a subject.
- A rhetorical analysis is based on examining the type of appeal to the audience, use of stylistic devices, and argumentation model employed by authors.
- A rhetorical analysis is performed in this section on ten samples drawn from diverse sources, including politicians, public servants, journalists, CEOs, academics, and computer scientists.
- The analysis finds that the samples rely on rhetorical devices and heuristics to convince the reader about the risks supposedly posed by cyber-security.
- The samples are convincing in their discussion about the vulnerabilities in our daily lives to cyber-crime and 'hacktivism.'
- The samples are not convincing in articulating the risks posed by cyber terrorism and cyber warfare, suggesting probability neglect is at play.

Rhetoric is a powerful tool that is often employed by management gurus. An example of a popular management tool using guru rhetorical techniques is Kaplan and Norton's *Balanced Scorecard*. First published in 1996, this well-known management tool claims to be a scientific way of reconciling financial and non-financial measures in accounting systems. Using a rhetorical analysis, however, Nørreklit (2003) found that the *Balanced Scorecard* relies on traditional guru techniques to make its appeal to its audience. Nørreklit's (2003) study will be used in this section to conduct a similar analysis of the cyber-security discourse.

Rhetoric involves stylistic devices and various types of arguments to develop a subject. The analysis of rhetoric is a combination of modernism and radical social constructivism. From this view, truth (or falsity) is attributed based on the "discursive practice or language game" employed by the source of the argument (Nørreklit, 2003, p. 593). From a radical social constructivist perspective, there are no universal standards of truth, meaning that one argument could be as good as any other. As such, all claims may be questioned; however, all claims are not equally sound. The question is whether an argument is convincing or simply persuasive.

Nørreklit (2003) structures her analysis of the *Balanced Scorecard* in three steps: its type of appeal to the audience, the stylistic devices it uses, and the argumentation model it employs:

- *Appeal to the audience* – There are generally three types of appeals to the audience: to the audience's *ethos* or trust in the credibility of the source, to the audience's *pathos* or emotions, or to the audience's *logos* or logic. The genre of text will typically influence the type of appeal used (p. 594-595).
- *Stylistic devices* – Popular tropes used in the guru field include analogies, metaphors, similes, metonymy, hyperbole, and irony. The lexis is also unique for its use of antithesis, loaded adjectives, and imprecise and intertextually based concepts (p. 599).
- *Argumentation model* – Arguments always include at least three basic elements: a claim, data, and a warrant. The *claim* refers to the point of view the source wishes the audience to accept. *Data* refers to the evidence the source uses to support the claim. Finally, the *warrant* is often implicit and combines the claim and data (p. 604).

This framework forms the basis of the rhetorical analysis used here on the cyber-security discourse. The analysis uses the following samples:

- *Cyber War: The next threat to national security and what to do about it* by Richard A. Clarke and Robert Knake (December 2010) – Introduction and Chapter 1
- "Cyber-attacks can spark real wars" by Richard Clarke, as first published in the February 16, 2012, edition of the *Wall Street Journal*
- "Canada's weakling Web defenses" by Misha Glenny, as first published in the May 18, 2011, edition of *The Globe and Mail*
- "The threat is real and must be stopped" by Joe Lieberman, as first published in the October 17, 2012, edition of *The New York Times*
- "Cyber guards or soldiers: which do we need most?" by Con Coughlin, as first published in the October 14, 2010, edition of *The Daily Telegraph*
- "Hire the hackers!" by Misha Glenny, a *TED Talk* delivered in July 2011
- "All your devices can be hacked" by Avi Rubin, delivered as a *TED Talk* in October 2011
- Nicholson, A., S. Webber, S. Dyer, T. Patel, H. Janicke. (2012). SCADA security in the light of cyber-warfare. *Computers and Security, 31*, 418-436.
- "Cybersecurity requires a multi-layered approach" by Laura Mather, as first published in the April 21, 2011, edition of *Info Security Magazine*
- "It's time to take cybersecurity seriously" by Tony Busseri, as first published in the March 12, 2012, edition of *Wired Magazine*.

It proceeds by analyzing the type of appeals to the audience, the stylistic devices employed, and the types of arguments used in the samples. Following the analysis, some broad observations will be made about the use of rhetoric as a tool in the cyber-security discourse.

Appeal to the audience

By far the most common type of appeal used in the sample is to the pathos or emotions of the audience. In fact, it is used to varying degrees in seven of the ten samples. The three samples that did not rely on an appeal to the emotions are the academic piece (Nicholson et al., 2012) and the two technical pieces (Mather, 2011; Busseri, 2012). The emotional appeals rest on common fears about technology. For instance, they note society's dependence on technology, the potential for digital devices to be infected with viruses without users' knowledge, and the possibility that sensitive information can be stolen or lost online (Clarke and Knake, 2010). References to infected devices as "zombies" give these fears an element of science fiction (Clarke and Knake, 2010; Glenny, May 2011).

There is another emotional element at play in many of these samples: the association of cyber-security with war and warfare. This association is created through frequent references to technology as a weapon, World War II, the Cold War, weapons of mass destruction, and the War on Terrorism (Clarke and Knake, 2010; Clarke, 2012; Coughlin, 2010; Nicholson et al., 2012). In these cases, technology is characterized as a new tool of modern warfare with effects as devastating as conventional or even nuclear warfare (Clarke, 2012; Coughlin, 2010). The support for this line of argument is the growing use of technology by other states, most notably China and Russia. Primarily, these state actors are shown to use technology to spy on Western governments and private businesses for the purposes of crime and industrial espionage.

However, several samples note instances in which technology was used as a form of conventional warfare.

Evidence of the use of technology for conventional warfare include the Stuxnet computer worm used by the United States and Israel to disrupt the Iranian nuclear program in 2010 and the use of technology by Russia in its 2008 conflict with Georgia (Clarke and Knake, 2010; Nicholson et al., 2012). Coughlin (2010) even begins his article with a hypothetical "clickskrieg" between Great Britain and China. These examples underscore technology's growing use for tactical purposes, using interference to disable communications and shut down the enemy's power systems. However, it is worth noting that the samples do not show technology as inflicting the same kinds of direct physical harm that could be compared with conventional weaponry or nuclear attacks. This fear is common in the cyber-security literature.

Furthermore, there is a sense throughout the samples that the West – especially the United States – is falling behind the technological capabilities of states like China and Russia. This reference recalls the arms race of the Cold War (Clarke and Knake, 2010; Coughlin, 2010; Glenny, May 2011, July 2011; Nicholson et al., 2012). Interestingly for Canadians, one case plays on the fear that Canada is at risk of losing its international reputation as a peaceful country because it houses several host servers that have run malicious programs (Glenny, May 2011).

There are also frequent links made between technology and terrorism, most commonly in the form of disruptions or attacks on critical infrastructure (Clarke, 2012; Glenny, July 2011; Lieberman, 2012; Nicholson et al., 2012). This argument notes only the potential for cyber-terrorism; in fact, there have yet to be any recorded incidents of cyber-terrorism (Clarke, 2012). As one case notes, terrorists may be interested in using technology for such purposes but they

currently lack the skills and capabilities required to launch such an attack (Nicholson et al., 2012).

In reality, few examples of real world cyber-terrorism given by the samples actually align with the literature's definition of terrorism. Only one case argues that technology has been used for ideological purposes, the component necessary to categorize an attack as a terrorist attack. Glenny (July 2011) argues that the hacker group Anonymous uses technology as a form of anarchism. It is worth noting that Anonymous has limited its actions to mischief thus far, a characteristic more in common with 'hacktivism' than cyber-terrorism. There is also only one case that gives evidence of technology being used to inflict direct physical harm. Rubin (2011) notes a study in which technological interference was used to disrupt pacemakers and disable the controls of automobiles. Nonetheless, these examples were the product of academic experiments conducted by computer scientists. Most of the discussion around cyber-terrorism therefore follows the critical literature's prediction that it is often confused with cyber-crime or 'hacktivism.'

While they rely mostly on pathos, the samples also display appeals to the audience's ethos (trust in the credibility of the source) and logos (logic), albeit to lesser degrees. Given the complexity of cyber-security issues, it is perhaps unsurprising that many of the authors have technical expertise in the field of computer science (Rubin, 2011; Nicholson et al., 2012; Mather, 2011; Busseri, 2012). However, the samples also feature current or former United States politicians and public servants with ties to national security (Clarke and Knake, 2010; Clarke, 2012; Lieberman, 2012). Joe Lieberman is the former chairman of the U.S. Senate Committee on Homeland Security and Governmental Affairs. Richard Clarke was a senior White House official and is now a lecturer at the Harvard Kennedy School of Government and an on-air consultant for

ABC News. The members of this latter category rely most on their credentials to advance their arguments. It is also interesting to note that both Lieberman and Clarke have non-partisan associations. Lieberman has served as a Democrat and an Independent, and worked closely with high profile Republicans such as John McCain. Meanwhile, Clarke has served in both Democratic and Republican administrations. This element of non-partisanship helps to give both authors an additional layer of credibility, making it appear as if they are writing without political bias.

In terms of logos, this type of appeal is most apparent in the academic article by Nicholson et al. (2012), the TED Talk by Rubin (2011), and the technical op-eds by Mather (2011) and Busseri (2012). While these pieces also argue that cyber-security is a threat, they primarily make their appeal by offering empirical evidence about the likelihood and impact of such attacks. They are also notable for clearly defining the ways in which technology can be used to initiate cyber-attacks. They accurately differentiate between 'hacktivism,' cyber-crime, and cyber-terrorism and offer technical solutions to combat future cyber-attacks.

By contrast, Clarke and Knake (2010), Clarke (2012), Coughlin (2010), and Glenny (May 2011, July 2011) accentuate the consequences of cyber-attacks and downplay their probability. They also rely on anecdotal evidence to advance their arguments. Furthermore, the authors frequently confuse cyber-warfare and cyber-terrorism with 'hacktivism' and cyber-crime. Finally, they offer vague solutions to thwart cyber-security threats. Indeed, these pieces are mostly used by the authors to raise awareness about the potential problems with cyber-security rather than to find solutions.

Nørreklit's (2003) observation that the genre of the text will influence the type of appeal might help to account for this discrepancy between technical experts and national security

specialists. Addressing an audience in an academic or technical medium may require a different type of appeal than addressing an audience in the popular press or at a TED Talk. However, it is interesting to note that while most of the samples use some type of emotional appeal to capture the audience's attention, the technical experts and national security specialists come to much different conclusions about what to do about cyber-security threats.

Stylistic devices

According to Nørreklit (2003), the management guru genre is unique for its use of tropes, such as analogies, metaphors, similes, metonymy, and hyperbole. It is also unique for its lexis, such as its use of antithesis, loaded adjectives, and imprecise and intertextually based concepts. The cyber-security literature analyzed here aligns with these predictions, particularly in its use of metaphors, antithesis, and irony. These three common stylistic devices will be described in detail next.

In terms of metaphors, the most predominant metaphor at use in the samples is the idea of cyberspace as a battlefield. Indeed, the idea of cyber-warfare is at play in all ten samples. From this perspective, information technology is a new weapon that can be wielded with devastating consequences. There is a clear difference between the depiction of cyber-warfare in the technical and popular pieces, however. In the technical pieces by Mather (2011) and Busseri (2012), the notion of cyber-warfare is used to explain common attacks on networked computers. The types of attacks the experts are most concerned about in these pieces are those typically emanating from hackers and cyber-criminals. The focus of these pieces is therefore to alert the technical community about emerging threats, draw attention to existing vulnerabilities, and to share best practices on how to detect and prevent cyber-attacks.

By contrast, the popular pieces are more concerned with technology being used for traditional terrorism purposes, such as attacking critical infrastructure. These samples also warn about the potential of technology to become incorporated into conventional warfare. This fear is played out to dramatic effect in the opening of Coughlin's (2010) article:

> The year is 2025, and the Royal Navy has just dispatched one of its new, state-of-the-art aircraft carriers to the Pacific Ocean, as a bitter trade dispute with China threatens to spill over into open conflict. Equipped with a full complement of Joint Strike Fighter warplanes, and escorted by a battle group of heavily armed destroyers and frigates, the carrier has been sent to demonstrate to Beijing that Britain is determined to protect international shipping lanes.
>
> Then, before a shot is fired in anger, the aircraft carrier and all the other ships are suddenly hit by a massive power failure. The engines and the computer systems shut down, and the fleet's powerful array of weaponry is rendered inoperable.
>
> At a stroke, the British battle group has been neutralised by teams of highly skilled computer hackers assigned to the People's Liberation Army (PLA), which have placed a computer worm in the fleet's operating systems.
>
> At the same time, Chinese cyber warriors launch a "clickskrieg" against mainland Britain. At the press of a mouse button, power stations, water firms, air traffic control and all government and financial systems are shut down. In the space of a few minutes, the entire nation has been paralysed. (Coughlin, 2010)

As this example demonstrates, the cyberspace-as-a-battlefield metaphor is a powerful stylistic device. It conveys the idea that technology is more than a tool of modern-day life. In this metaphor, technology has the potential for serious and even sinister purposes. This idea is played out by likening the destructive potential of technology to other well-known incidents, such as World War II, Pearl Harbor, the Cold War, or September 11th. Recalling the power of the availability heuristic, this metaphor creates a powerful association between technology and other traumatic events, making it seem as if technology could wreak the same devastating consequences. As a result, the samples call for action to prevent such catastrophes in the future,

even when they offer little to no empirical evidence of technology actually being used for such purposes.

The use of antithesis is also prevalent in these samples and is connected to the battlefield metaphor. The contrast between conventional warfare and cyber-warfare used in Coughlin (2010), for example, recalls the contrast between the industrial age and the information age used in the *Balanced Scorecard.* The contrast between conventional warfare and cyber-warfare makes it seem as if cyber-warfare is replacing conventional warfare. This depiction creates the sense that we are at a revolutionary moment in time. It also perpetuates the idea that cyber-warfare is somehow different and more advanced than conventional warfare, and that relying exclusively on conventional warfare for security is now obsolete. Using antithesis, therefore, the samples can suggest that cyber-warfare is the way of the future, and that those who do not adapt to the new paradigm risk being left behind. This exaggeration causes the audience to overestimate the necessity of implementing cyber-warfare techniques and adopting cyber-defenses.

Finally, the use of irony is prevalent in some samples as well. This stylistic device is used in a few ways. As Clarke and Knake (2010) note, for instance, the United States created the Internet but is now more vulnerable because of it. They argue that the United States can never truly keep its cyber-security defenses up-to-date because of the rapid pace of technological innovation and change. Therefore, irony is used to justify the ongoing need for cyber-security solutions, invoking a perpetual mission to improve cyber-security that can never truly end.

Argumentation model

Finally, the samples display some of the argument models profiled by Nørreklit (2003). The most prevalent argumentation model used in the samples typically follows this pattern:

- Claim: Country A is vulnerable to cyber-attacks.
- Data: Cyber-attacks can be devastating and disruptive.

- Warrant: Country A is vulnerable to devastating and disruptive cyber-attacks.

This logical fallacy is often used to make the argument that, because a certain country experiences cyber-attacks and some cyber-attacks can be devastating and disruptive, then all cyber-attacks that country will experience must be devastating and disruptive. The problem with this reasoning is that it ignores the extremely low probability that a devastating and disruptive cyber-attack will occur, influencing the audience to believe that the threat is more extreme than evidence would suggest.

Another prevalent argumentation model used in the sample is *argumentum ad populum*, a common logical fallacy that appeals to the authority of the many in order to prove a claim (Cathcart and Klein, 2007). Many of the samples use this logical fallacy to argue for improved cyber defenses. For example, Glenny (May 2011) argues that Canada needs to have a government-run computer emergency response team because, after all, "it is the only major Western country not to have one." In other words, if every other country is doing it, Canada should as well. Glenny (July 2011) uses this line of argument later in order to argue that Western countries should hire hackers to run their computer security systems because countries like Russia and China have already recruited them.

This logical fallacy is used by the samples to encourage countries that are supposedly lagging behind in cyber-security – such as the United States (Clarke and Knake. 2010), the United Kingdom (Coughlin. 2010), and Canada (Glenny. May 2011) – to develop better cyber-defenses. However, just because some countries are pursuing cyber-defenses does not necessarily make it a good idea for all countries to do so. This argumentation model is therefore fundamentally flawed.

As this section has demonstrated, the samples from the cyber-security discourse employ persuasive rhetorical techniques to advance their arguments. Applying Nørreklit's (2003) framework uncovers many common rhetorical tools at play, such as appealing to the audience's fear of terrorism and nuclear war, exaggerating the necessity of implementing cyber-security solutions, and arguing using common logical fallacies.

Interestingly, this analysis has found that the samples align with other predictions of the literature as well. In terms of the psychology literature, the availability heuristic was found to be at play in the way that the samples create associations between technology and catastrophic events like terrorist attacks. In terms of the critical cyber-security literature, many of the samples also confuse cyber-terrorism with 'hacktivism' and cyber-crime. These findings are therefore in line with many of the literature's predictions.

The samples also show that traditional management guru techniques are being used to overdramatize and oversimplify the cyber-security problem. The samples do succeed in making the argument that the spread of technology has introduced new vulnerabilities into our daily lives. This argument is most convincingly made by the academic piece (Nicholson et al., 2012), the TED Talk by a computer scientist (Rubin, 2011), and the technical pieces (Mather, 2011; Busseri, 2012). However, the types of vulnerabilities that appear to be most frequent and probable are those emanating from hacktivists and cyber-criminals. The argument about the dangers of cyber-terrorism and cyber-warfare is not as sound.

The samples that do warn about the dangers of cyber-terrorism and cyber-warfare use traditional management guru techniques to make their case (Clarke and Knake, 2010; Clarke, 2012; Glenny, May 2011, July 2011; Lieberman, 2012; Coughlin, 2010). This trend is seen in their arguments' contradictory nature, instability, use of recycled ideas, and reliance on soft data

and logic – four of the six features of guru theories identified by Hood and Jackson (1991). As such, it is possible that the dangers of cyber-terrorism and cyber-warfare cited in these samples are indeed being overdramatized using traditional guru techniques.

It is also worth noting, however, that 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 (Quigley, 2013). As such, reliable information on the frequency and severity of attacks is not always easy to come by. Inquiring with cyber-security practitioners directly – as the last section of this project does through a series of qualitative interviews with practitioners in Canada and the United Kingdom – is one way to address this problem.

6.0 Interview findings

Section summary

- People working in different public sector contexts understand cyber-security differently.
- Cyber-technology offers flexibility and innovation in service delivery but introduces risks to information security, especially from information kept on mobile devices. When considering these risks, decision-makers are aware of both the likelihood and consequences of a cyber-security breach.
- The media play a role in bringing some issues/trends about cyber-security to people's attention but decision-makers about cyber-security in public sector organizations tend to be influenced most by peer networks.

This section presents the findings from interviews about cyber-security with decision-makers from public sector organizations.

6.1 Findings

The main findings have to do with: 1) how the interview participants conceptualize/think about cyber-security, 2) the risks and benefits they perceive to be associated with using cyber-technology in their organizations, and 3) how they find out about cyber-security issues and the extent to which they are influenced by the media. Each of these findings is discussed in turn below.

What is cyber-security?

This sub-section considers how decision-makers about cyber-security from universities, government, and public healthcare conceptualize cyber-security. It also presents the views of a private sector cyber-security consultant in this respect.

Universities. Within the context of a university, participants from universities in Canada and the UK shared a similar understanding of cyber-security. They thought that cyber-security is about "protecting information owned by the university or used by the university" but it is also about "protecting individuals within that university."

One interviewee thought the term cyber-security was dated. To this participant, cyber-security has evolved over the past ten years to become more about data protection than protection against hackers, malware, and viruses. These interviewees also used the terms "information" and "data" interchangeably but distinguished information as being "contextualized data" such as a student's grades. They expressed similar views that "information security is about the availability, integrity, and confidentiality of your information." The participants seemed to suggest that they recognized that people's perceptions of privacy are changing and that this will have an impact on what information people want protected.

Government and public healthcare. The two participants from a Canadian provincial government agreed that cyber-security had to do with complying with relevant legislation and policy. They were concerned especially with the Freedom of Information and Protection of Privacy (FOIPOP) Act.

A participant from a Canadian municipal government thought that cyber-security was about defending and maintaining control of the municipality's systems. He explained that this could be anything from preventing vandalism of a municipality webpage, to protecting information about undercover police operations, to maintaining control of infrastructure like water, wastewater, and traffic signals systems.

Compared to other public services, protection of privacy was not seen as important for municipal government. The participant from municipal government stated that most of the municipality's data are publicly accessible and that the worst breach of privacy could come from the hacking of property tax bills. He did stress that unauthorized modification of publicly accessible data was a risk he had to manage.

In UK public healthcare, cyber-security was thought to be "about protecting patients' privacy, the information in their medical records". To put this statement in context, many UK health boards are now using electronic medical records instead of paper ones.

Private sector cyber-security consultancy. The private sector cyber-security consultant stated that cyber-security "means many things" and that "the classic buzz words [used regarding cyber-security] are confidentiality, integrity, and credibility."

The consultant's expertise is in "preventing sabotage and impairment of the systems controlling critical infrastructure, such as the power system, water purification, chemical plants, [and] refineries." He stated that his clients' primary concerns about cyber-security relate to safety. For example, "Don't kill my employees. Don't put the public safety at risk. Don't cause an environmental catastrophe." His clients' secondary concerns about cyber-security relate to reliability. For example, "Do not impair the operation of my typically multi-billion dollar physical asset that, frankly, the business and to some extent society depends on." He reiterated that the priorities for cyber-security are "safety first, reliability second."

The main finding in this sub-section is that cyber-security means different things to people depending on the context in which they work. Across these contexts, three themes emerged: 1) protection of privacy, 2) protection/integrity of information, and 3) protection of systems/assets.

Risks and benefits

This sub-section considers the risks and benefits that cyber-security decision-makers in universities, government, and public healthcare perceive from using cyber-technology in their organizations.

Universities. Participants from Canadian and UK universities expressed very similar perceptions about the risks and benefits associated with using cyber-technology. They recognized that universities are open environments where people share information and that "you can put in information security measures [to control this but] you would stop a lot of what goes on in a university if you did that. We're not a bank; we shouldn't operate like that."

While one of the main benefits to universities of cyber-technology is greater ease of information sharing, participants agreed that "the largest risk is people ... what people do." For example, regarding the use of email, "people can be very resistant to changing their passwords regularly, not writing their passwords down, not sharing their passwords with other people ... and this has resulted in the university being blacklisted[1] for sending out spam email.".

Participants agreed that another major risk to cyber-security is from Bring Your Own Device (BYOD) (i.e. the use and loss of mobile devices like laptop computers, tablets, and even mobile phones). "If someone lost their unencrypted laptop, then again, almost certainly there is a potential disclosure of that data. Now it wouldn't definitely be there but you were asking about the potential, and if people had details of their students, details of their research, details of some business contracts that they're involved in, you'd be losing information that's confidential, sensitive, or commercially valuable through a lost device. So at the moment it's almost 100 per cent that if a device is lost then there is a risk of an information security breach. It doesn't mean that there will definitely be one; perhaps the device will just be re-formatted."

One risk identified by the participant from the Canadian university was people's use of free web-based services like Dropbox and Google Docs. He recognized the resource and cost implications for the university providing those types of services. The use of free web-based

[1] Blacklisting is the refusal of one email system to accept email from another system because it has been identified as a sender of spam. This usually occurs after a computer has been compromised or taken over by a third party.

services was not a concern for participants from the UK university because they have web-based access to their university server. Despite this, "you wouldn't believe the number [of people who] keep their information on their C: drive. You remember [fire in university building] ... there were hundreds of devices that had to be cleaned. Now it costs more to clean a laptop after a fire than it costs to buy you a new laptop ... so every one you cleaned had vital information on it.... You'd have destroyed them had you not needed to get the information off of them ...so hundreds and hundreds of them where people needed to get the information back and they must have been weeks and weeks without their information because there were a lot of them to be cleaned, they took a long time to be cleaned, they couldn't just be switched on because even to run them for a small number of time, the corrosive nature of the soot on the device would have destroyed it before we got the information off it. So, you had there an information security risk, so information security affects the availability of your data, the confidentiality of your data, the integrity of your data...so we had hundreds and hundreds of them to be cleaned there because people had their entire life history of their research from the past 20 years on their laptop."

Government and public healthcare. Participants from government noted that the biggest cyber-security risk is the protection of privacy. One participant noted that legislation prohibits government from storing personal information on servers outside Canada. He considered this with respect to address books on mobile devices that may go through iCloud to servers in the United States and whether disabling iCloud on mobile devices would severely decrease their functionality.

The participant from municipal government reported that councillors want to use mobile devices to interact with their constituents on social media sites like Facebook and Twitter. He recognized that this introduced new risks but felt it was important to find a balance between

managing those risks and gaining benefits from councillors being more accessible to the public. Innovation and benefits were also perceived with respect to municipal government offering open data so that other organizations could use it to make money and offer services that the municipal government does not currently provide.

In UK public healthcare, the use of electronic patient records has "created new risks for protecting patients' privacy." It has, however, led to increased patient safety. For example, "if a patient attends A&E [accident and emergency, the UK equivalent of the Emergency Room] their electronic record is readily available ... and clinicians will know what medications they're on ...and can avoid administering double doses [of medications]." An emerging issue is information ownership, especially with respect to adverse incident data. "With the introduction of electronic adverse incident recording and reporting systems ... it has become easier to collect and collate data about adverse incidents ... and patients are increasingly demanding access to this data ... [but] this has facilitated organizational learning."

The main finding from this sub-section is that cyber-technology makes it easier to share data and that can lead to benefits of faster and more flexible ways of working, and improved service delivery. These benefits need to be balanced, though, against the risks to protection of privacy from information kept on mobile devices, and on computer servers outside of organization or home country. When considering these risks, decision-makers are aware of the likelihood of a cyber-security breach as well as the consequences.

Information seeking and the media

This sub-section considers how cyber-security decision-makers in universities and government learn about cyber-security issues and the extent to which they are influenced by the media. It also presents the views of a private sector cyber-security consultant in this respect.

Universities. The participant from the Canadian university stated that major newspapers give him a broad overview of relevant issues. He mentioned listservs and blogs as other information sources but noted that these sources sometimes contained more noise than information and so he tended to rely on an informal network of peers and colleagues.

Participants from the UK university stated that they received cyber-security information mainly from Janet (Joint Academic Network)[2], UCISA (University and Colleagues Information Systems Association), and HEIDS (Higher Education Information Directors of Scotland). These organizations were considered to be "highly trustworthy" as they "are unlikely to have any other agenda", especially Janet as it is "government-owned" and aims to provide a network infrastructure that meets the needs of UK universities. "My staff and other IT directors" were identified as other trusted sources of cyber-security information. The BBC (British Broadcasting Corporation) was identified as a prominent news source but was thought to be "quite superficial" in terms of reporting cyber-security issues but probably "fairly accurate".

Government and public healthcare. Participants from Canadian government and UK public healthcare agreed that they were informed about cyber-security issues through peers. For example, the participant from municipal government stated that he was a member of the Association of Municipal Administrators and trusted his peers from that organization with respect to cyber-security issues. Participants also agreed that they do not trust major newspapers to report the details of cyber-security issues accurately and were skeptical of computer magazines due to their commercial interests.

Private sector cyber-security consultancy. The private sector cyber-security consultant stated that his "employer is spending a great deal of time on face-to-face marketing and so I

[2] https://www.ja.net/

attend a great many conferences. I hear about these issues face-to-face with customers and other vendors in those contexts." He stated that he also reads material from the Digital Bond blog "pretty religiously... I follow a handful of experts on Twitter and I read the Register just to keep up with general security issues and whether control issues, cyber-security issues hit the mainstream press. I look at the most technical of the mainstream press."

With respect to trust in these information sources, the participant stated that he "contribute[s] to some of these sources from time to time. I am a writer so I have an insider's knowledge of what goes into publishing on this topic and so I take everything with a grain of salt. So I don't know about trust. When possible, I will use those sources to learn about topics of interest. I will dig into the topics if I'm interested in them and try to find the original sources and make my own assessment of what's real and what's not."

The main finding from this sub-section is that organizational decision-makers about cyber-security are informed and influenced most by peer networks. While the popular media plays a role in bringing cyber-security issues to people's attention, it was seen as too lacking in technical details to be influential.

7.0 Conclusion

This was a brief study conducted during a short time frame. As such, there are important methodological constraints to acknowledge. First, due to the limited time available, we were only able to interview a small number of subjects. In order to ensure that our findings from this small sample would be representative, we only interviewed *public sector* managers. They were sampled from different regions and different public sector organizations and the interviews were designed to be inductive and exploratory. Despite these limitations, common themes emerged from the interviews, which were reinforced by our literature review and aspects of our rhetorical analysis. Based on this, we make some recommendations, but also call for further research on the themes we discuss here. We outline a future research agenda at the end of the executive summary and the conclusion.

The discussion around cyber-security is about the risks associated with the Internet; this is a highly uncertain risk. New pervasive technologies pose new threats and opportunities for society; those with power can often be threatened by these new technologies because it is unclear how they will change power structures in society. Katzenbach (1973), for example, explains generals' reluctance to replace horses in military operations with trucks and tanks in the early part of the 20th century as an expression of the generals' fears over their relative inexperience with the new technology. Notwithstanding their capacity to bring about significant change, technologies do not always change power structures significantly; powerful institutions tend to re-exert their control over technologies and in fact use the technologies to further their particular agenda.

It is also not unusual to see private markets respond quickly to exploit the uncertainty of risks associated with new technologies in order to sell their wares. In the run-up to Y2K, we saw

the industry persuade owners and operators of critical infrastructure to identify, fix, test, and audit all mission critical systems before January 1, 2000. The cost of Y2K is counted in the trillions of dollars (Quigley 2008). In this case, the organizational design of bureaucracies did not help. Public bureaucracies tend to segment and specialize responsibilities, which made it difficult to get an overall view of the risk. Equally, its tendency to use a standard approach made it difficult to prioritize systems and accept some level of risk for lower priority systems.

Cyber-security issues have crept into our everyday lives, but few people actually understand them. This discrepancy has left policy-makers, the media, and the public vulnerable to exploitation by cyber-security gurus. As this study has shown, persuasive IT specialists can exploit this knowledge gap and manipulate others into believing that the threats posed by information technology are imminent and dire, even without offering sound evidence to justify such a claim.

The first part of this report focused on ways in which persuasive cyber-security gurus manipulate popular fears about information technology for their own gain. It did so by borrowing from the psychology-of-risk, management-guru, and critical cyber-security literature. The psychology literature illustrated how people are affected by cognitive biases such as heuristics. Heuristics were shown to lead people into believing hazards are more probable or extreme than they actually are. On a related note, management gurus have also been shown to use rhetoric to achieve the same effect: they focus largely on consequences of extreme events and tend to omit or overlook probabilities. Management gurus have typically targeted the field of business and management to sell their ideas. With the advent of information technology, however, they have been presented with a new and timely medium to exploit. This trend has been accentuated by a concurrent growth in the fear of cyber-terrorism and cyber-warfare.

As the rhetorical analysis section indicated, cyber-security threats have become intricately entwined with broader hazards such as warfare and terrorism. The result is that the public has become sensitive to threats with a defense or terrorism element, even when there is little evidence to support these fears. Aided by expert knowledge, the use of rhetorical techniques, and the presence of cognitive biases like heuristics, cyber-security gurus were shown to have a distinct advantage over laypersons.

In the second part of the paper, we report on the results of our interviews with cyber-security decision-makers in public organizations. These decision-makers do not seem to be influenced by the rhetoric of cyber-gurus. Rather, they report that they use peer networks to find information and stay informed because they trust their peer networks for reliable information and common sense checks. Our interview subjects were largely concerned with privacy and data integrity issues, particularly for publicly available information. This focus is likely influenced by the relevant legislation that guarantees the protection of information. Perhaps to the chagrin of the cyber management gurus, our research suggests that terrorism, sabotage, and vandalism of web pages were not concerns of these public sector managers.

Recommendations

IT public sector managers belong to peer-networks within public services; these networks are based on trusting interpersonal relationships. Public sector organizations should recognize the importance of these peer-networks for managing cyber-security risks and develop and support them.

Institutional arrangements should reinforce the importance of cyber-security. The interviews revealed that some IT managers thought that cyber-security was a shared responsibility between IT and the people who are using the organization's IT systems and information. While sharing responsibility for critical resources is laudable, public agencies must actively promote responsible IT security behaviours among the staff and clarify roles and responsibilities lest the ambiguity over responsibility become an opportunity for blame-shifting between parties when things go wrong. Each public organization should also have a highly visible and accessible "cyber-security champion" who promotes awareness of cyber-security issues. This appointment will not only bring attention and resources to the subject, but will also provide a reliable internal resource that can offset the potentially powerful influence of external IT consultants whose incentives are not necessarily aligned with the public organization's goals.

Governments should be more specific about the terms they use to describe breaches in cyber-security. We discuss four types in this paper: cyber-crime, 'hacktivism,' cyber-terrorism, and cyber-warfare. The perpetrators of each are driven by different motives and the solutions to each will also be different. Equally, public officials should be mindful of the metaphors they employ. Our research suggests that the metaphor of cyber as a 'battlefield,' for example, is overused and is often inaccurate. The metaphor implies that the risk should be understood in terms of survival as opposed to a trade-off between costs and benefits; this distinction has a potentially powerful impact on the manner in which one approaches a risk problem.

Indeed, government officials must develop a more nuanced understanding of risk. Our comments here are constrained somewhat due to the fact that reliable information related to cyber-warfare and cyber-terrorism is not easily available. Neither industry nor government readily disclose such information (Quigley 2013). That noted, the rhetorical analysis section

demonstrates that management consultants emphasize extreme consequences and either overlook, suppress or exaggerate probabilities depending on the point the consultants wish to make. When, for instance, should government strategies and operations be guided by 'worst case scenario' thinking? Precautionary approaches to managing risks are expensive (Sunstein, 2005). Taking a precautionary approach with a specific risk includes a price in terms of opportunity cost, and inevitably increases other (often less visible) risks, intentionally or unintentionally. What is the potential opportunity cost of not having progressive social media policies that allow public servants to engage with the citizenry in online fora, for instance? Government must develop a more effective method to prioritize systems and the security required for such systems. Sunstein (2009) advises that we should consider catastrophic and irreversible harms – particularly to human and environmental safety – as the risks that require a more cautious approach and have a more balanced approach with the others. Interview subjects reinforced this observation.

Relatedly, we may be at a point where the very notion of privacy must be reconsidered. Interview subjects noted that certain information is protected but it need not be, or at least not to the standard to which it presently is: people's expectations about what should be private are changing. There are potentially significant resource and democratic implications to keeping information private. We need to have a better understanding of what really needs to be protected to a high level and what does not. Public bureaucracies are susceptible to regulating in the face of uncertainty; over-regulating information availability jeopardizes the potential innovation and transparency of public institutions.

Government must acquaint itself with an industry perspective in order to communicate more effectively with industry. Government interests and practices at times differ from those of industry. As one interview subject noted, strategists for national defense, for instance, often interpret risks in terms of its capacity to withstand an attack from an enemy. In this calculation, survival is always paramount. When the survival of an organization is at stake, risk can no longer be described as the product of probability and expected monetary losses. In the case of national defense, there is at times a disproportionate focus on consequence with relatively less focus on probability. In contrast, industry balances dangers with financial opportunities. Industry is not necessarily interested in international espionage or cyber-warfare; it is often more interested in insider threats, extortion, industrial espionage, intellectual property, the protection of financial data and learning best practices from others in its sector. To assist industry, government can help to facilitate the exchange of information and establishment of standards in these areas in particular.

Government must also understand the needs of the public. Consumers of government services expect to be able to use a variety of mobile devices to find information specific to their needs (Flumian, 2009). Politicians often support these initiatives on behalf of their constituents and moreover, would like to engage with their constituents on one of a number of devices and on one of a number of social media sites. Mobile devices and the fusion of data represent increased opportunities and risks. While there may be some exceptions, such as identity theft, the research we conducted suggests that the public is not particularly concerned about many aspects of cyber-security. Meeting this demand for flexibility—from the public and the elected officials—will continue to exert pressure on public officials with responsibility for cyber-security.

Most cyber events lack the characteristics of a 'good' media story (e.g., 'catching a bad guy') and therefore tend not to be included in popular media coverage (Fowler and Quigley, nd). Lately, we have seen a rise in coverage of cyber bullying. Child abuse – whether cyber or not – generates considerable media coverage and it can often be highly emotionally charged (Hood, Rothstein and Baldwin, 2001; Fowler and Quigley, nd). The government needs to use these types of events to raise awareness, not in an anxiety-generating way but rather to encourage a more sophisticated understanding of risks associated with the Internet in a manner in which people can identify in their personal lives. Some have argued that cyber-security is a civic duty (Harknett and Stever, 2009) though to date this argument has failed to take hold. More education in schools and at home about cyber risks will enhance our understanding of the issues. In turn, this focus will allow people to better protect themselves and also contribute to policy discussions about what level of risk we are prepared to tolerate in cyber-space, and how active the government should be in this policy area.

These recommendations are really just the beginning of this strategy; how to think about the cyber space is a long term proposition. If we think about the environmental movement, for example, it took decades to arrive at our present policies. Indeed, recall Carson's landmark environmental publication *Silent Spring* was published just over fifty years ago. It is remarkable to think that we now recycle to the degree that we do as a matter of course. Cyber needs to go undergo this same transformation.

In fact, rather than a battlefield, it might be more appropriate to think of cyber-space as the American Wild West – a place of little regulation and considerable opportunity and risk. All of our critical assets depend on the successful functioning of the Internet: supply chains depend

on it; children play on it; adults shop on it. Still, unlike any other critical system upon which society depends, it exists largely without safeguards. In the same way that regulation in aviation or medicine enhances its value to the community, cyber-space might also (ultimately) benefit from such regulation and education. It will require a public that is better informed of the risks and opportunities of the Internet. A strong education program that engages the public might in the long term lead to the behavior change required to ensure that the benefits of cyber-space are maximized and its dangers reduced. This strategy will enhance personal responsibility, but will also carve out an appropriate role for government in protecting critical infrastructure and vulnerable populations.

Recommended next steps for this research

As noted, the interview study was based on a small sample of public sector managers. We recommend conducting a larger-scale interview study with participants from both the public and private sectors. This would allow for comparison of how public and private sector managers monitor the external environment for emerging cyber-security threats and opportunities, and a comparison of best practices between the sectors. It would also be useful to compare how owners and operators of large critical infrastructure entities such as healthcare and power supply perceive cyber risks with small and medium-sized operators, such as those found in the manufacturing and agricultural sectors.

Finally, we believe it is also important to explore issues of diversity. White males, non-white males, and women typically receive, process, and act on risk messages differently (see, for example, Finucane et al., 2000; Flynn et al., 1994). As email, texting and social media become

the communication tools of choice, we believe it is crucial to explore how this affects online behavior and perceptions of risk.

8.0 Appendix I: Interview Schedule

1. What does cyber-security mean to you?

2. Tell me about cyber-security in your organization.

3. Tell me what you know about (cyber-security issue). What is (e.g. the Cloud)? How does (e.g. the Cloud) work?

4. How do you find out about cyber-security issues?

5. Tell me about your trust in those information sources.

6. Tell me about your trust in technology at your workplace for cyber-security.

7. How risky do you think (cyber-security issue) is?

8. How do you balance the opportunities (e.g. innovation, efficiencies) and risks of cyber-technology?

9. In general, what cyber-security issue stands out most in your mind? How likely do you think this issue is to occur? Why do you think this issue stands out in your mind?

10. What about (other cyber-security issues from question 1 that participant has not been mentioned)?

11. What lesson do you think your organization needs to learn about cyber-security?

Appendix II: Interview methodology

The people interviewed for this study were mainly decision-makers about cyber-security from public sector organizations in Canada and the UK. Three participants were from universities (1 Canada, 2 UK), three were from Canadian government (2 provincial, 1 municipal), and one was from a public healthcare organization in the UK. One private sector cyber-security consultant (based in Canada) was also interviewed in order to offer a broader perspective on the issues.

The research protocol, including the interview schedule (see Appendix I), was approved by a departmental ethics committee at the University of Strathclyde, UK. Apart from one interview (the two provincial government employees were interviewed together), the interviews were carried out on a one-to-one basis either by telephone or at the interviewee's place of work. A researcher from Dalhousie University, Canada, interviewed Canadian participants, and a researcher from the University of Strathclyde, UK, interviewed British participants. The interviews lasted between 45 and 90 minutes.

Appendix III: Rhetorical analysis methodology

The samples were chosen based on their publication date (between 2010 and 2012), the medium in which they were published, and their relevance to the project at hand. Efforts were made to collect samples from a variety of sources, including the popular media, from technical experts, and from academia. Not surprisingly, the authors of these pieces come from diverse fields, representing politicians, public servants, journalists, CEOs, academics, and computer scientists.

The limits of this analysis include the size of the sample, the sampling method used, and the collection of the data. The limited number of cases used here (n=10) impacts the generalizability of this study. The sampling method, a nonprobability method called 'quota sampling,' also influences the results. Using 'quota sampling,' the population of cyber-security discourse was separated into distinct and mutually exclusive categories or sub-groups. Judgment was then exercised by the researchers to select samples from each sub-category according to pre-determined proportions. In other words, selection of the data was non-random.

The benefits of this method are that all relevant categories were covered and there was greater variability in the samples than random sampling can sometimes achieve. The downside of this method is that a subjective judgment was made by the researchers about which samples to include in the study. The potential issue with this approach is that researchers may choose cases that appear to support their hypothesis and exclude those that do not. While this problem is indeed a valid concern, 'quota sampling' is the most appropriate method for this project. The project is primarily interested in how rhetoric is being used by cyber-security gurus, not how often. While that topic is out of the scope of this project, it would be a fruitful topic for future research.

9.0 Works cited

Ahonen, A. and T. Kallio. 2009. "On the cultural locus of management theory industry: Perspectives from autocommunication." *Management and Organizational History* (Vol. 4, No. 4), 427-443.

Berglund, J. and A. Werr. 2000. "The invincible character of management consulting rhetoric: How one blends incommensurates while keeping them apart." *Organization* (Vol. 7, No. 4), 633-655.

Burns, C. 2012. "Implicit and explicit risk perception." Paper presented at the European Academy of Occupational Health Psychology (Zurich).

Busseri, T. (12 March 2012). It's time to take cybersecurity seriously. *Wired Magazine.*

Cathcart, T. and D. Klein. 2007. *Aristotle and an aardvark go to Washington: Understanding political doublespeak through philosophy and jokes* (New York: Abrams Image).

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* (Vol. 4, Issue 1), 19-36.

Clark, T. and G. Salaman. 1996. "The management guru as organizational witchdoctor." *Organization* (Vol. 3, No. 1), 85-107.

Clark, T. and G. Salaman. 1998. "Telling tales: Management gurus' narratives and the construction of managerial identity." *Journal of Management Studies* (Vol. 35, No. 2), 137-161.

Clarke, R. (16 February 2012). Cyber-attacks can spark real wars. *The Wall Street Journal*.

Clarke, R. A. and R. Knake. 2010. *Cyber War: The next threat to national security and what to do about it.* (Toronto: Harper Collins Canada).

Colarik, A. and L. Janczewski. 2012. "Establishing Cyber Warfare Doctrine." *Journal of Strategic Security* (Vol. 5, No. 1), 31-48.

Coughlin, C. (14 October 2010). Cyber guards or soldiers: Which do we need most? *The Daily Telegraph.*

Faisal, M. N., D. K. Banwet and R. Shankar. 2006. "Supply chain risk mitigation: Modeling the enablers." *Business Process Management Journal* (Vol. 12, No. 4), 535-552.

Finch, P. 2004. "Supply chain risk management." *Supply Chain Risk Management: An International Journal* (Vol. 9, Issue 2), 183-196.

Finucane, M. L., P. Slovic, C.K. Mertz, J. Flynn, and T.A. Satterfield. 2000. "Gender, race, and perceived risk: The 'white male' effect." *Health, Risk and Society* (Vol. 2, No.2), 159-172.

Flumian, M. 2009. Citizens as prosumers: The next frontier of service innovation. Ottawa. Retrieved on March 24, 2013, at http://iog.ca/publications/citizens-as-prosumers-the-next-frontier-of-service-innovation/

Flynn, J., P. Slovic, and C.K. Mertz. 1994. "Gender, race, and perception of environmental-health risks." *Risk Analysis.* (Vol. 14, No.6), 1101-1108.

Fowler, T. and K. Quigley. nd. "Contextual Factors that Influence the Canadian Government's Response to the Cyber Threat." Under Review.

Glenny, M. (18 May 2011). Canada's weakling Web defenses. *The Globe and Mail.*

Glenny, M. (July 2011). Hire the hackers! *TED Talks.* Retrieved online from: http://www.ted.com/talks/misha_glenny_hire_the_hackers.html

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

Harknett, R. J. and J. A. Stever. (2009). "The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen". *Journal of Homeland Security and Emergency Management* (Vol. 6, Issue 1).

Hood, C. and M. Jackson. 1991. *Administrative Argument* (Sudbury, MA: Dartmouth Publishing).

Hood, C., H. Rothstein, and R. Baldwin. 2001. *The government of risk: Understanding risk regulation regimes.* (Oxford: OUP).

Huczynski, A. 2006. *Management gurus: Revised edition* (New York: Routledge).

Jaeger, C. C., O. Renn, E. A. Rosa, and T. Webler. 2001. *Risk, uncertainty, and rational action.* (London: Earthscan Publications).

Katzenbach, E. L. 1973. "The Horse Cavalry in the Twentieth Century." *Readings in American Foreign Policy: A bureaucratic perspective.* (Boston: Little Brown).

Keulen, S. and R. Kroeze. 2012. "Understanding management gurus and historical narratives: The benefits of a historic turn in management and organization studies." *Management and Organizational History* (Vol. 7, No. 2), 171-189.

Kieser, A. 1997. "Rhetoric and myth in management fashion." *Organization* (Vol. 4, No. 1), 49-74.

Kolluru, R. and P. H. Meredith. 2001. "Security and trust management in supply chains." *Information Management and Computer Security* (Vol. 9, Issue 5), 233-236.

Lewis, J. 2003. "Cyber terror: Missing in action." *Knowledge, Technology, and Policy* (Vol. 16, No. 2), 34-41.

Lieberman, J. (17 October 2012). The threat is real and must be stopped. *The New York Times.*

Mather, L. (21 April 2011). Cybersecurity requires a multi-layered approach. *Info Security Magazine.*

Moore, M. 1995. *Creating public value.* (Cambridge, MA: Harvard University Press).

Nicholson, A., S. Webber, S. Dyer, T. Patel, and H. Janicke. (2012). SCADA security in the light of cyber-warfare. *Computers and Security* (Vol. 31), 418-436.

Nørreklit, H. 2003. "The Balanced Scorecard: What is the score? A rhetorical analysis of the Balanced Scorecard." *Accounting, Organizations and Society* (Vol. 28), 591-619.

Osborne, D., and T. Gaebler. 1992. *Reinventing government: How the entrepreneurial spirit is transforming the public sector.* (Reading, MA: Addison-Wesley).

Quigley, K. 2008. *Responding to crises in the modern infrastructure: Policy lessons from Y2K.* (Palgrave Macmillan)

Quigley, K. 2013. "'Man Plans, God Laughs': Canada's National Strategy for Protecting Critical Infrastructure." *Canadian Public Administration.* (Vol. 56, No. 1).

Røvik, K. A. 2011. "From fashion to virus: An alternative theory of organizations' handling of management ideas." *Organization Studies* (Vol. 32, No. 5), 631-653.

Rubin, A. (October 2011). All your devices can be hacked. *TED Talks.* Retrieved online from: http://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked.html

Sjöberg, L. 2000. "Factors in risk perception." *Risk Analysis* (Vol. 20, No. 1), 1-11.

Slovic, P., B. Fischhoff, and S. Lichtenstein. 1979. "Rating the risks." *Environment* (Vol. 21, No. 3), 14-20.

Slovic, P., B. Fischhoff, and S. Lichtenstein. 1982. "Why study risk perception?" *Risk Analysis* (Vol. 2, No. 2), 83-93.

Slovic, P., E. Peters, M.L. Finucane, and D.G. MacGregor. 2005. "Affect, risk, and decision making." *Health Psychology.* (Vol. 24), S35-S40.

Smith, D. and J. McCloskey. 1998. "Risk and crisis management in the public sector: Risk communication and the social amplification of public sector risk." *Public Money and Management* (Vol. 18, No. 4), 41-50.

Stohl, M. 2006. "Cyber-terrorism: A clear and present danger, the sum of all fears, breaking point, or patriot games?" *Crime, Law, and Social Change* (Vol. 46), 223-238.

Sunstein, C. 2003. "Terrorism and probability neglect." *Journal of Risk and Uncertainty* (Vol. 26, No. 2), 121-136.

Sunstein, C. 2005. *Laws of fear: Beyond the precautionary principle.* (New York: Cambridge University Press).

Sunstein, C. 2009. *Worst case scenarios*. (Cambridge, MA: Harvard University Press).

Werr, A. and A. Styhre. 2003. "Management consultants: Friend or foe? Understanding the ambiguous client-consultant relationship." *International Studies of Management and Organization* (Vol. 32, No. 4), 43-66.

Yould, R. E. 2003. "Beyond the American fortress: Understanding homeland security in the information age." In *Bombs and bandwidth: The emerging relationship between*

information technology and security, ed. Robert Latham. (New York: The New Press), 74-97.