‘Cyber Gurus’: A Rhetorical Analysis of the Language of Cybersecurity Specialists and the Implications for Security Policy and Critical Infrastructure Protection

Abstract

This paper draws on the psychology of risk and "management guru" literature (Huczynski, 2006) to examine how cybersecurity risks are constructed and communicated by cybersecurity specialists. We conduct a rhetorical analysis of ten recent cybersecurity publications ranging from popular media to academic and technical articles. We find most cybersecurity specialists in the popular domain use management guru techniques and manipulate common cognitive limitations in order to over-dramatize and over-simplify cybersecurity risks to critical infrastructure (CI). We argue there is a role for government: to collect, validate and disseminate more data among owners and operators of CI; to adopt institutional arrangements with an eye to moderating exaggerated claims; to reframe the debate as one of trade-offs between threats and opportunities as opposed to one of survival; and, finally, to encourage education programs in order to stimulate a more informed debate over the longer term.

Keywords

Cybersecurity, risk perception, availability heuristic, management gurus, rhetoric, critical infrastructure

1.0 Introduction

There is a tension at the centre of our relationship with technology. On the one hand, there is incredible optimism that information technology can simultaneously improve service delivery and cut costs (Layne & Lee, 2001; Sharif, 2008). On the other hand, there is burgeoning IT security literature that warns that our increasing dependence on technology is becoming a liability because the technology can be so easily attacked by those with malicious intent, and the critical infrastructure and services that depend on it can be so easily discontinued (Clarke & Knake, 2010). Our paper is particularly interested in the latter claim. Much of the research on computer security and critical infrastructure protection, however, focuses on the ways in which organizations secure their networks and information in the supply chain (Kolluru & Meredith, 2001; Faisal, Banwet & Shankar, 2006; Von Solms & Van Niekerk, 2013). Less attention has been paid to how organizations construct and understand cybersecurity risks. Our failure to do so constitutes a risk in itself. It is not enough for systems to be secure; they have to seem secure (Bertot, Jaeger & Grimes, 2010).

There are three purposes to this paper. The first is to provide an understanding of how cybersecurity risk is constructed. We will draw on the psychology of risk literature to show that people have numerous biases that prevent them from drawing reliable inferences in the face of uncertainty. Following this, we examine 'management gurus' literature, which explains how consultants, academics and authors who profit from selling solutions to complex organizational issues persuade audiences of the usefulness of their ideas. Secondly, we use the techniques Nørreklit (2003) employed in her rhetorical analysis of *The Balanced Scorecard* to analyze cybersecurity discourse in ten recent publications. The publications range from popular print media to TED Talks to academic and technical articles. We are particularly interested in

examining the extent to which cybersecurity specialists are using management guru techniques and manipulating common cognitive limitations in order to over-dramatize and over-simplify cybersecurity risks.

Finally, using a cybernetic understanding of control (information gathering, standard setting and behaviour modification), we examine the policy challenges that emerge as a result of the present framing of cybersecurity risks. The ultimate goal will be to question the effectiveness of how we talk about and raise awareness of cybersecurity issues in general and what policies we should adopt to address potential weaknesses in governance of cyberspace that are aggravated further by the present cybersecurity discourse.

2.0 The Psychology of Risk and the Techniques of Management Gurus

2.1 The psychology of risk

Burns (2012) argues it is important to understand risk perception for two reasons. First, risk perception helps us to understand and predict people's behaviour. Secondly, awareness of how perceptions are constructed helps to improve communication between technical experts and laypersons. The psychometric paradigm draws on the work of cognitive psychologists such as Slovic, Fischhoff and Lichtenstein (1982) to conceptualize risks as personal expressions of individual fears or expectations. In short, individuals respond to their perceptions whether or not these perceptions reflect reality. The study of risk perception has grown significantly over recent decades and has constituted a significant challenge to rational actor approaches to risk (see for example Pratt, 1964; Arrow, 1971; Slovic, 1987; Jaeger, Renn, Rosa & Webler, 2001; Pennings & Grossman, 2008; Lachlan & Spence, 2010; Pachur, Hertwig & Steinmann, 2012). The

psychology of risk literature has identified several biases in people's ability to draw inferences in the face of uncertainty. Risk perception can be influenced by properties such as personal control (Langer, 1975), familiarity (Tversky & Kahneman, 1973), exit options (Starr, 1969), equitable sharing of both benefits and risks (Finucane, Slovic, Mertz, Flynn & Satterfield, 2000) and the potential to blame an institution or person (Douglas & Wildavsky, 1982). It can also be associated with how a person feels about something, such as a particular technology or a disease (Alhakami & Slovic, 1994). People also show confirmation bias (Wason, 1960), which suggests they seek information to confirm how they feel, not to challenge it.

A central finding of the risk perception literature is that perceptions are often, in fact, faulty, when we consider consequence *and* probability (Slovic *et al*., 1982). Risk cannot be directly observed; rather, it is constructed by people based upon their understanding of hazards in everyday life. People often make judgments about risk using incomplete or erroneous information. They also rely on judgmental biases or heuristics to comprehend complexity. Heuristics are cognitive tools people use to analyze risk and complexity (Slovic *et al*., 1982). In some ways, they are helpful; heuristics allow people to render simplistic understandings of complicated subjects. However, they can also oversimplify or distort our understanding. Heuristics fall along two primary dimensions: the unknown factor and the dread factor. The unknown factor influences people to be more concerned with risks that are not observable or known to science (Slovic *et al*., 1982). On the other dimension, the dread factor influences people to be more concerned with risks that are not controllable and pose potentially catastrophic consequences (Slovic *et al*., 1982).

One of the most common heuristics is *availability.* Under the influence of the availability heuristic, people tend to believe that an event is more likely to occur if they are able to imagine

or recall it easily (see for example Slovic, Fischhoff & Lichtenstein, 1979; Folkes, 1988; Betsch & Pohl, 2002; Tversky & Kahneman, 1973; Maldonato & Dell'Orco, 2011). For instance, 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 suddenly 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, such as in the workplace or the home. Availability is considered to be one of the most important heuristics for understanding risk perception (Sjöberg, 2000). For instance, the availability heuristic influences people to be concerned about terrorist attacks despite the fact that – like other many high-profile risks – it is considered to be extremely unlikely (Gierlach, Belsher & Beutler, 2010). This phenomenon is referred to as 'probability neglect' (Slovic, Peters, Finucane & Macgregor, 2005). 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). In other words, people tend to overemphasize the consequences of risks while minimizing or even ignoring the probabilities.

2.2 Management gurus

The term 'management guru' refers to the authors, publishers, editors, consultants, managers, commercial seminar organizers and professors who offer advice on business and management (Kieser, 1997). The field is primarily 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.

There are three key themes in the management guru literature: how guru ideas become popularized, their unique appeal to managers and common techniques.

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). Finally, 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 &

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 & Kallio, 2009, p. 433). As such, the search for the best management ideas serves a therapeutic role for 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).

The literature also accounts for how popular management ideas become influential. One of the fundamental findings is that rhetoric is a common and influential technique. For example, Hood and Jackson (1991) argue that persuasion fuels organizational change more often than objective facts. In their view, speakers attempt to establish their theories as the most credible, not necessarily the most truthful. To this end, Hood and Jackson (1991) identify six salient features of administrative arguments: 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 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 contrast to the theoretical knowledge offered by academics. This positioning lends management gurus affinity with managers as 'one of us' (Huczynski, 2006). Government 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 & Gaebler, 1992; see also Moore, 1995; Osborne & Plastrik, 1997).

Management guru techniques and heuristics are powerful tools. The psychology-of-risk literature and management guru literature are connected to this study by the way gurus are able to overdramatize or oversimplify complex organizational issues. Their objective is to inspire managers – usually using rhetorical arguments – to implement their solutions to solve complex organizational problems. Often these problems are based on issues related to the efficiency, success or welfare of an organization. As the next section will demonstrate, these themes are also prevalent in the cybersecurity discourse.

3.0 Rhetorical analysis: Cybersecurity discourse examined

3.1 Depictions of cybersecurity threats

From a risk governance perspective, cybersecurity threats might usefully be described as "uncertain risks" (Renn 2008). Uncertain risks occur where there is "a lack of clear scientific or technical basis for decision making." In other words, we often lack reliable empirical data to estimate with confidence the probability and consequence of the risk. This limitation diminishes the confidence level of traditional objective measures of risk estimation and becomes more reliant on "fuzzy" or subjective measures of risk estimation (Renn 2008: 18-19). As a result, these risk events can generate 'surprises' or realizations that are not anticipated or explained explicitly within a risk modeling framework.

Despite the increase in popular discourse about cybersecurity, there is reason to be careful about over-estimating the probability of the risks and to ensure we understand the

motivations behind different actions. Today, there are four main depictions of threats in the cybersecurity literature:

- *Cyber-terrorism* – 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, 2007, p. 229). Cyber-terrorism means that these acts are committed using technology.
- *'Hacktivism'* – Refers to "the marriage of hacking with political activism" (Stohl, 2007, p. 236).
- *Cyber-crime* – Refers to criminal offenses committed on-line or through other forms of information technology.
- *Cyber-warfare* – Refers to "the role of information technology as an enabler of warfare" (Colarik & Janczewski, 2012, p. 39).

While these are four prevalent types of cybersecurity issues, there is evidence to suggest that the threat is exaggerated and oversimplified for some. Many note the lack of empirical evidence to support the widespread fear of cyber-terrorism and cyber-warfare, for instance (Lewis, 2003; Stohl, 2007; Cavelty, 2007; Hansen & Nissenbaum, 2009; Rid, 2013).

According to Stohl (2007), there is little vulnerability in critical infrastructure that could lead to violence or fatalities. Secondly, there are few actors who would be interested in or capable of exploiting such vulnerabilities. Thirdly, and in relation to cyber-terrorism in particular, 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, 2007). 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, 2007, p. 230).

By contrast, 'hacktivism' is much more common. 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, 2007, 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 rather than to cause violence or death. Cyber-crime is also a major issue, but more problematic in terms of law enforcement and business (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 either overshadowed by or misrepresented as cyber-terror. This representation has the effect of increasing awareness of high impact/low probability threats such as cyber-terrorism while more common forms of cybersecurity risk like 'hacktivism' or cyber-crime and the sources of these more common problems receive less attention.

3.2 Rhetorical analysis of the cyber discourse

3.2.1 Rhetorical analysis methodology

Based on Nørreklit's (2003) rhetorical analysis of the argumentation in Kaplan and Norton's *The Balanced Scorecard*, we structure our analysis according to the categories below.

- *Appeal to the audience* – appeal 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

(Aristotle & Kennedy, 1991). The genre of text will typically influence the type of appeal used.

- *Stylistic devices* – use of popular tropes used in the guru field including analogies, metaphors, similes, metonymy, hyperbole, irony, antithesis, loaded adjectives and imprecise and intertextually-based concepts.
- *Argumentation model* – involves three basic elements: a claim, data and a warrant (Walton, 1996). 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 (Nørreklit, 2003).

Table 1: Cases

Author(s)	**Date published**	**Title**	**Type**	**Country**
Richard A. Clarke & Robert Knake	December 2010	Cyber War: The Next Threat to National Security and What to Do About It (Introduction & Chapter 1)	Book (Non-fiction)	United States
Richard Clarke	February 16, 2012	Cyber-attacks can spark real wars	Newspaper article (*Wall Street Journal*)	United States
Misha Glenny	May 18, 2012	Canada's weakling web defenses	Newspaper article (*Globe and Mail*)	Canada
Joe Lieberman	October 17, 2012	The threat is real and must be stopped	Newspaper article (*New York Times*)	United States
Con Coughlin	October 14, 2010	Cyber guards or soldiers: Which do we need most?	Newspaper article (*Daily Telegraph*)	United Kingdom
Misha Glenny	July 2011	Hire the hackers!	Ted Talk (Journalist)	United States
Avi Rubin	October 2011	All your devices can be hacked	Ted Talk (Academic)	United States

Nicholson, Webber, Dyer, Patel & Janicke	2012	SCADA security in the light of cyber-warfare	Scholarly article	United Kingdom
Laura Mather	April 21, 2011	Cyber-security requires a multi-layered approach	Technical magazine (*Info Security Magazine*)	United States
Tony Busseri	March 12, 2012	It's time to take cyber-security seriously	Technical magazine (*Wired Magazine*)	United States

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 study at hand. Efforts were made to collect samples from a variety of sources, including the popular print media, from technical experts and from academia. 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 sample size, the sampling method, and the collection of the data. The 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 cybersecurity 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 predetermined 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 the researchers may have inadvertently chosen cases that appear to support their hypothesis while excluding those that do not. While this problem is indeed a valid concern, 'quota sampling' is the most appropriate method for this paper. The paper is primarily interested in whether rhetoric is being used by

cybersecurity specialists and in which ways. While this is an initial study into the use of management guru techniques in cybersecurity, a larger study would be a fruitful topic for future research.

3.2.2 Results

Appeal to the audience

The most common type of appeal used in the sample is to pathos; seven of the ten samples use it. The three academic/technical pieces did not (Nicholson, Webber, Dyer, Patel & Janicke, 2012; Mather, 2011; Busseri, 2012). There are several emotional appeals at play. The first is based on fears about people's lack of control and technology's potential to cause catastrophe, both themes that generate negative risk perceptions according to risk psychology literature. For instance, some of the samples note the potential for digital devices to be infected with viruses without users' knowledge, and the possibility that sensitive information can be stolen or lost on-line (Clarke & Knake, 2010; Glenny, May 2011). The articles conflate the characteristics of living and non-living entities in order to convey, on the one hand, a sinister and motivated entity and, on the other hand, an entity that has immediate global reach and is indifferent to inflicting human suffering or financial loss. This is captured most effectively in the description of "zombies." (See Table 2.)

Table 2: Computers as 'Zombies': Living and non-living characteristics, focussed on destruction

Author (s)	**Examples**
Clarke and Knake (2010)	"Sometimes the zombie computer sits patiently waiting orders. Other times it begins to look for other computers to attack. When one computer spreads its infection to others, and they in turn do the same, we have the phenomenon known as a 'worm,' the infection worming its way from one computer through thousands to millions. An infection can spread across the globe in mere hours" (p. 14).

Glenny (May 2011)	"A bedrock of cybercriminality is the 'distributed denial of service' attack, in which tens of thousands of zombie computers enslaved by viruses to a command-and-control machine will lay siege to a company's or organization's system."

Four of the samples associate cybersecurity with warfare (see Table 3), which the risk-psychology literature indicates generates high dread. Technology is characterized as a tool of modern warfare with effects as devastating as conventional or even nuclear warfare (Clarke, 2012; Coughlin, 2010). There are several references to technology as a weapon, World War II, the Cold War, weapons of mass destruction, and the "War on Terror" (Clarke & Knake, 2010; Clarke, 2012; Coughlin, 2010; Nicholson *et al*., 2012). China and Russia in particular are shown to use technology in clandestine ways, such as for spying on Western governments and private businesses for the purposes of crime and industrial espionage. Three samples note instances in which technology was used as a form of conventional warfare as well (Clarke & Knake, 2010; Coughlin, 2010; Nicholson *et al.*, 2012).

Table 3: Cyberspace as 'battlefield' is a common metaphor

Author (s)	**Examples**
Clarke and Knake (2010)	"In anticipation of hostilities, nations are already 'preparing the battlefield.' They are hacking into each other's networks and infrastructures, laying in trapdoors and logic bombs – now, in peacetime. This ongoing nature of cyber war, the blurring of peace and war, adds a dangerous new dimension of instability" (p. 31).
Coughlin (2010)	"But there is also a growing body of opinion, within both military and intelligence circles, that future threats are as likely to take place in cyber space as on the battlefield."
Nicholson *et al.* (2012)	"It is understood that attacks and defence issued by nation states take place over networks rather than by physical means such as army personnel, vehicles and barracks" (p. 421).

Further evidence of the use of technology for conventional warfare includes 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 & Knake,

2010; Nicholson *et al*., 2012). Coughlin (2010) begins his article with a hypothetical "clickskrieg" between Great Britain and China, an example we analyze further in the stylistic devices section. These examples emphasize the use of technology to disable communications and power systems on a large scale. The samples do not, however, show technology inflicting the direct physical harm that could compare with conventional weaponry or nuclear attacks. Furthermore, there is a sense that the West – especially the United States – is falling behind the technological capabilities of countries like China and Russia (see Table 4), which recalls the arms race of the Cold War (Coughlin, 2010; Glenny, May 2011; Glenny, July 2011; Nicholson *et al*., 2012).

Table 4: Cold War Parallels: Russia and China are most advanced and should be feared

Author (s)	**Examples**
Coughlin (2010)	"On the one hand, there is the danger posed by countries such as China, which has invested enormous resources in trying to use the internet to infiltrate Western governments and institutions, in order to acquire information on military capabilities and sensitive commercial information that can be used to Beijing's advantage."
Glenny (May 2011)	"After all, you never know whether your hacker is working for Russian organized crime, an Indian manufacturer, or the People's Liberation Army. Relative to other Western countries, Canada's cyberdefences lack funding and a coherent strategy."
Glenny (July 2011)	"In China, in Russia and in loads of other countries that are developing cyber-offensive capabilities, this is exactly what they are doing. They are recruiting hackers both before and after they become involved in criminal and industrial espionage activities -- are mobilizing them on behalf of the state. We need to engage and find ways of offering guidance to these young people, because they are a remarkable breed."
Nicholson *et al*., 2012	"As was demonstrated by the Chinese and Russian spies in Gorman (2009) it is clear that other nations are perpetrators and their reasons include industrial espionage and military purposes. As evidence is beginning to show, these actions demonstrate that elements of future wars are likely to be fought in cyberspace" (p. 422).

Finally, there are also associations made between technology and terrorism, often in the form of attacks on critical infrastructure (see Table 5) (Clarke & Knake, 2010; Clarke, 2012; Glenny, July 2011; Lieberman, 2012; Nicholson *et al*., 2012; Coughlin, 2010; Busseri, 2012). Yet the cases only cite the potential for cyber-terrorism; in fact, there have yet to be any recorded incidents on this scale (Clarke, 2012). As one author notes, terrorists may wish to use technology for such purposes but they currently lack the skills (Nicholson *et al*., 2012).

Table 5: Critical infrastructure depicted as vulnerable

Author (s)	**Examples**
Clarke and Knake (2010)	"If they take over a network, cyber warriors could steal all of its information or send out instructions that move money, spill oil, vent gas, blow up generators, derail trains, crash airplanes, send a platoon into an ambush, or cause a missile to detonate in the wrong place."
Clarke (2012)	"If the hackers turn their attention to disruption and destruction, as some have threatened, they are likely to find the controls for electric power grids, oil pipelines and precious water systems inadequately secured. If a hacker causes real physical damage to critical systems in that region, it could quickly involve governments retaliating against each other with both cyber and conventional weapons."
Lieberman (2012)	"The threat of a cyber attack on our electric grid, water supply system, financial networks, or oil and gas lines is anything but hype. I have been concerned about this threat for years, and the evidence has grown exponentially that sophisticated adversaries could paralyze the nation with targeted cyber attacks on critical networks."
Nicholson *et al*. (2012)	"Whilst none of these incidents have been officially reported as attacks on SCADA systems they demonstrate the dependence of critical infrastructure on these systems and illustrate the widespread impact that could occur should an attack on a critical infrastructure take place. The possible damage that such a cyber attack could cause is comparable to that of a physical attack such as 9/11" (p. 423).
Coughlin (2010)	"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."

Few examples of cyber-terrorism align with the literature's definition of terrorism. Only one case argues that technology has been used for ideological purposes, a necessary feature of a

terrorist attack. Glenny (July 2011) argues that the hacker group Anonymous uses technology as a form of anarchism. 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 but in these cases they were computer scientists' experiments. Most of the discussion of cyber-terrorism therefore follows the critical literature's prediction that it is often confused with cyber-crime or 'hacktivism.'

The samples also display appeals to the audience's ethos (trust in the credibility of the source) and logos (logic). Given the complexity of cybersecurity 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). The samples also feature current or former United States politicians and public servants with experience in national security (Clarke & Knake, 2010; Clarke, 2012; Lieberman, 2012) and bipartisanship, such as Joe Lieberman and Richard Clarke. These qualities help to establish credibility.

Logos 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 cybersecurity is a threat, they primarily make their appeal by offering empirical evidence about the likelihood and impact of such attacks. They also define the ways in which technology can be used to initiate cyber-attacks, accurately differentiating between 'hacktivism,' cyber-crime and cyber-terrorism. Finally, they offer technical solutions to combat future cyber-attacks.

By contrast, Clarke and Knake (2010), Clarke (2012), Coughlin (2010), and Glenny (May 2011, July 2011) emphasize the consequences of cyber-attacks and attenuate their probability. They also rely on anecdotal evidence to advance their arguments and frequently conflate cyber-

warfare and cyber-terrorism with ‘hacktivism’ and cyber-crime. Finally, they offer vague solutions to thwart cybersecurity threats. Indeed, the authors of these pieces raise awareness about the potential problems with cybersecurity rather than offer solutions.

Stylistic devices

The cybersecurity literature analyzed here uses metaphors, antithesis and irony, in particular. These three common stylistic devices will be described in detail.

The most predominant metaphor at use in the samples is the idea of cyberspace as a battlefield (see Table 3). 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 are those 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 good 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 (see Table 4). 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 . . . 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).

In this metaphor, technology has the potential for serious and sinister purposes. This idea is reinforced through other pieces, 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 an association between technology and well known traumatic events, making it seem as if technology could cause the same consequences. While the samples call for action to prevent such catastrophes, they offer little to no empirical evidence that technology can be used for such purposes.

The use of antithesis is also prevalent in four samples, three of which use the battlefield metaphor (Clarke & Knake, 2010; Clarke, 2012; Coughlin, 2010; Rubin, 2011). The contrast between conventional warfare and cyber-warfare used in Coughlin (2010), for example, gives the impression that cyber-warfare is replacing conventional warfare. This depiction conveys the notion that we at a critical moment in time – that cyber-warfare is somehow different and more advanced than conventional warfare, and that relying exclusively on conventional warfare is misguided and in fact creates important vulnerabilities.

Finally, the use of irony is prevalent in six of the samples. This stylistic device is used to argue that people have benefited from advances in information technology but are now more vulnerable because of it as well. Individuals, governments and organizations can never truly keep their cybersecurity defenses up-to-date because of the rapid pace of technological innovation and change and that it is fully embedded in our society (Clark & Knake, 2010; Glenny, May 2011, July 2011; Lieberman, 2012; Mather, 2011; Busseri, 2012). Therefore, irony is used to justify the ongoing need for cybersecurity solutions, invoking a perpetual mission to improve cybersecurity that can never end.

Argumentation model

The samples display three common logical fallacies. The first is inductive argument. Clarke and Knake (2010) argue that because a certain country experiences devastating and disruptive attacks, then all cyber-attacks will be devastating and disruptive. The argument ignores probabilities. Four samples use the second logical fallacy, *argumentum ad populum*, which is an appeal to the authority of the many (Cathcart & Klein, 2007; Clarke & Knake, 2010; Glenny, May 2011, July 2011; Coughlin, 2010). Glenny (May 2011), for example, argues that Canada needs to have a government-run computer emergency response team because "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) also argues that Western countries should hire hackers to run their computer security systems because countries like Russia and China have already recruited them. The third logical fallacy, which is present in two samples, is implicit warrant. Clarke (2010), for example, argues that if something is old, it must be of no use. Glenny (May, 2011) employs an implicit warrant when he argues that, first, because Canada's computer energy response centre guards the country's critical national infrastructure, it needs to be "in government hands" and, secondly, because it involves national security, Canada's military should manage cybersecurity. Table 6 summarizes our findings.

Table 6: Summary of key findings ('√' is a check mark; it indicates 'present' or 'affirmative')

Case	Appeal to Audience	Stylistic Devices	Argumentation Model
Cyber War Richard A. Clarke & Robert Knake (2010)	Ethos ∨	Metaphor ∨	Inductive argument ∨
	Logos	Antithesis ∨	Argumentum ad populum ∨
	Pathos ∨	Irony ∨	Implicit warrant
Cyber-attacks can spark real wars Richard Clarke (2012)	Ethos ∨	Metaphor ∨	Inductive argument
	Logos	Antithesis ∨	Argumentum ad populum
	Pathos ∨	Irony	Implicit warrant ∨

Canada's weakling web defenses Misha Glenny (May 18, 2011)	Ethos	Metaphor ∨	Inductive argument
	Logos	Antithesis	Argumentum ad populum ∨
	Pathos ∨	Irony ∨	Implicit warrant ∨
The threat is real and must be stopped Joe Lieberman (2012)	Ethos ∨	Metaphor ∨	Inductive argument
	Logos	Antithesis	Argumentum ad populum
	Pathos ∨	Irony ∨	Implicit warrant
Cyber guards or soldiers: Which do we need most? Con Coughlin (2010)	Ethos	Metaphor ∨	Inductive argument
	Logos	Antithesis ∨	Argumentum ad populum ∨
	Pathos ∨	Irony	Implicit warrant
Hire the hackers! Misha Glenny (July 2011)	Ethos	Metaphor ∨	Inductive argument
	Logos	Antithesis	Argumentum ad populum ∨
	Pathos ∨	Irony ∨	Implicit warrant
All your devices can be hacked Avi Rubin (2011)	Ethos	Metaphor ∨	Inductive argument
	Logos ∨	Antithesis ∨	Argumentum ad populum
	Pathos ∨	Irony	Implicit warrant
SCADA security in the light of cyber-warfare Nicholson *et al.* (2012)	Ethos	Metaphor ∨	Inductive argument
	Logos ∨	Antithesis	Argumentum ad populum
	Pathos	Irony	Implicit warrant
Cyber-security requires a multi-layered approach Laura Mather (2011)	Ethos	Metaphor ∨	Inductive argument
	Logos ∨	Antithesis	Argumentum ad populum
	Pathos	Irony ∨	Implicit warrant
It's time to take cyber-security seriously Tony Busseri (2012)	Ethos	Metaphor ∨	Inductive argument
	Pathos	Antithesis	Argumentum ad populum
	Logos ∨	Irony ∨	Implicit warrant

The analysis found that the samples align with many of the predictions of the literature. The availability heuristic was found to be at play in the way that the samples create associations between technology and high dread events like terrorist attacks. Many of the samples also conflate cyber-terrorism with 'hacktivism' and cyber-crime. The samples also show that traditional management guru techniques are being used to overdramatize and oversimplify the cybersecurity problem. The academic piece (Nicholson *et al*., 2012), the TED Talk by a computer scientist (Rubin, 2011), and the technical pieces (Mather, 2011; Busseri, 2012) succeed in making the argument that technology has introduced new vulnerabilities into our lives. However, the types of vulnerabilities that appear to be most frequent are those emanating from

'hacktivism' and cyber-crime. The arguments about the dangers of cyber-terrorism and cyber-warfare are less compelling.

The samples warning about the dangers of cyber-terrorism and cyber-warfare use traditional management guru techniques to make their case (Clarke & 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 administrative arguments 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.

4.0 Discussion: Policy Implications

A cybernetic understanding of control points to three components in a control system: information gathering, standard setting and behaviour modification. If any of its three components is absent, a system is not considered to be in control in a cybernetic sense (Hood, Rothstein & Baldwin, 2001, pp. 23-25). In this section we apply this lens to understand better the weaknesses in the risk regulation regime that governs cybersecurity and critical infrastructure, and the importance of framing the debate properly in order to address these weaknesses.

Information Gathering

Bertot *et al.* (2010) argue that transparency and the right to access government information are now internationally regarded as essential to democratic participation and trust in government. There is an absence of reliable information, however, on cybersecurity risks and recorded attacks. When information *is* available, there is a lack of reliable probability data that can place such events in the appropriate context. The few incidents that are public knowledge –

such as the 2010 Stuxnet attack on Iranian nuclear facilities, for example – are often sensational, catastrophic and amplified in military terms by cyber specialists in the popular media. As a result, cyber-threats can be misunderstood as military or terrorist attacks rather than more mundane – yet commonplace – threats to business operations such as 'hacktivism' or cyber-crime.

When it comes to critical infrastructure, many Western countries put considerable emphasis on information sharing. (See, for example, Public Safety Canada, 2009; Australia's Attorney-General's Department, 2003; United Kingdom: Centre for the Protection of National Infrastructure, 2006; United States: Department of Homeland Security, 2008). Nevertheless, years after 9/11 many of these goals continue to be aspirational (Dearstyne, 2005; Gordon, 2010); governments continue to have a patchwork of information-sharing policies (Strickland, 2005; Paquette, Jaeger & Wilson, 2010). Information sharing with respect to national security is constrained by a number of issues, including complexity and uncertainty (Renn, 2008), legal barriers (Quigley, 2013; Shore, 2008), capacity to share, institutional culture (Baker, 2010; Hood, 1998; Relyea, 2004), secrecy and, in the case of the private sector, which owns and operates most of the critical infrastructure, competition (Quigley & Mills, 2014). Industry leaders are reluctant to discuss the vulnerabilities of assets because of the risk to their organization's security, liability, share value and public image (Quigley, 2013).

Developing trust within and between the public and private sectors is cited frequently in the Western governments' CIP strategies noted above as a way to address these issues. Although social scientists have given considerable attention to the problem of defining trust, a concise and universally accepted definition remains elusive. As a consequence, the term 'trust' is used in a variety of distinct and not always compatible ways in organizational research (Rousseau, Sitkin,

Burt & Camerer, 1998; Kramer, 1999; Barbalet, 2009; Hardin, 2006; Quigley, 2013). While most governments refer to trusted *partnerships* with industry, in many cases they may actually be referring to *dependencies*. Government takes risks when it aspires to be seen as a 'trusted partner' in this context. CI and emergency events can result in clashes over public and private sector accountability structures (Koliba, Mills & Zia, 2011; Koski, 2011). Industry responds to its shareholders and is rewarded for taking successful risks. Government has a regulatory role to play on behalf of citizens to ensure appropriate adherence to standards. Strengthening the relationships between government and industry can produce stability and collegiality among regulators and CI owners and operators, but may also result in compromises on transparency and prevent dramatic changes, if required (Vogel, 1986).

Governments should therefore strengthen their role in the risk regulation regime, including in collecting, validating and disseminating information. Timely and actionable intelligence can allow CI owners, operators and managers to adapt according to their own needs and circumstances. Government should support a Knowledge Commons (Hess & Ostrom, 2007; Comfort, 2010); it includes a shared knowledge base and it requires infrastructure and organizational processes to support information search, exchange, updates, storage and transmission. Sector networks provide value to private industry. By exchanging ideas on 'good practices' in their sectors and lessons identified from previous failures, organizations can learn about what is working without having to discuss their vulnerabilities. Non-disclosure agreements and anonymized information can usefully facilitate learning opportunities. If the claims of the cyber specialist are indeed exaggerated, a more reliable information-gathering regime will help to expose this. At a minimum they will have either to reconsider their arguments or provide more convincing evidence.

Government itself is not without credibility issues, however. Polling in most Western countries suggests that trust in government is in decline (Edelman, 2013). In this sense, in trying to build up trust with CI owners and operators, government might be going in the wrong direction. Rather, it should try to build up trust among citizens in government's ability to regulate CI and those responsible for it. After all, critical infrastructure is not critical just for industry but for society as a whole. Ironically, most national strategies on critical infrastructure are completely silent on citizen engagement and outward accountability. While private firms will want to ensure their information is protected to a degree, this protection will have to be balanced with more outward accountability to ensure trust between governments and the citizenry grows in this policy area.

Standard Setting

Governments should be more specific about the terms they use to describe breaches in cybersecurity. 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 have access to different resources; the probability that each will occur is different; 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 inaccurate. The metaphor implies that the risk should be understood in military terms and chiefly as one 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. When the survival of the firm is at stake, risk can no longer be described as the product of probability and expected monetary losses. A more appropriate description in these cases can be attempted in

terms of cardinal utilities (Jaeger *et al*., 2001). This extreme position is rarely the case with critical infrastructure, however. For the most part, owners and operators of CI balance threats with opportunities. Industry is not immediately concerned with the traditional concerns of departments of defense, such as in international espionage or warfare. Rather, industry is more concerned, as Lewis (2003) points out, about insider threats, extortion, industrial espionage, intellectual property, the protection of financial data and learning good practices from others in its sector.

A market approach to critical infrastructure protection, however, has challenges. While standing at the ready for low-probability/high-consequence events can rarely be justified in market terms, failure to do so creates risk not only for the firm itself but for all those who depend on it. In a highly interdependent and just-in-time context, the cost of failure can be considerable for the supply chain or, indeed, the community as a whole. Public safety is a public good; the costs associated with cybersecurity are susceptible to the problems of moral hazards and freeriding. This suggests vulnerabilities will persist. Government officials must develop a more nuanced understanding of risk. Many of the popular pieces we examined emphasize extreme consequences and overlook, suppress or exaggerate probabilities depending on the point the authors wish to make. Not all risks are equal. When, for instance, should government strategies and operations be guided by 'worst case scenario' thinking? Precautionary approaches to managing risks are expensive, if not at times illogical and contradictory (Sunstein, 2005). There are also opportunity costs. Government policies that ban staff from using social media for security reasons, for instance, prevents public servants from engaging in relevant and important popular discourse that concern their policy areas (Roy, 2012; Fyfe & Crookall, 2010; Conabree, 2011).

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 one that is balanced with the others. More reliable data will help us to distinguish higher consequence risks from lower ones. Government must tolerate some level of risk with some systems, however, otherwise innovation will be stifled. The absence of data that can help officials to be more specific about the magnitude of the risk require that CI owners and operators avoid high vulnerability as best as they can, develop flexible responses to cope with surprises and a diversity of means to accomplish mission-critical tasks. They also need to continue to gather reliable data and monitor the current state of risk.

Behaviour Modification

A major determinant in the successful adoption of e-government is acceptance of ICTs by public servants and the public (Bertot *et al.*, 2010). Cyber is still in its infancy. We need to support a learning culture (Senge, 1990) underpinned by more reliable data collection, and the use of more appropriate metaphors and framing techniques to explain the nature of cyber-threats to laypersons. This learning culture needs to be upheld by the institutional arrangements. IT security professionals must be represented at senior administrative levels within governments and CI organizations to offer more neutral expert opinions to counter inflated cyber rhetoric. Managers frequently rely on each other for quality information and support in understanding cybersecurity threats (Quigley, Burns & Stallard, 2013). These formal and informal networks should be actively supported and encouraged within organizations and across communities of practice (Agranoff, 2008). Public agencies and organizations that operate the CI upon which society depends should be subject to audits to ensure they are meeting reasonable standards

according to their industry. We must also increase the pool of reliable information by declassifying more information (Quigley, 2009; Gordon, 2010) and encouraging greater cooperation between military and civilian operations in order to develop a more nuanced understanding of risks, as opposed to more extreme ones characterized by many cybersecurity specialists (Mittu *et al*., 2008).

These recommendations are really just the beginning of this strategy; how to think about cyberspace is a long-term proposition and must involve the public. Most cyber security failures, , such as credit card fraud, 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 & Quigley, 2014; Quigley & Mills, 2014). Lately, we have seen a rise in coverage of cyber bullying (Smith & Steffgen, 2013). Child abuse – whether cyber or not – generates considerable media coverage and it can often be highly emotionally charged (Hood *et al*., 2001; Fowler & Quigley, 2014). The government needs to use these types of events to raise awareness, not in an anxiety-generating way but rather to encourage a better understanding of risks associated with the Internet that emphasizes probability not just consequence, and the reasonable steps one can take to protect oneself. In so doing we can employ heuristics to characterize cyber risks as risks that affect people in their everyday lives, which are much more likely to be criminal acts or mischief, not warfare, and that these risks require an approach that balances opportunities with threats. Some have argued that cybersecurity is a civic duty (Harknett & 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 cyberspace, and how active the government should be in this policy area.

5.0 Conclusion

The uncertainty of potential cyber security events has left policy-makers 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 claims. Uncertain risks can generate surprises or realizations that are not anticipated or explained explicitly within a risk modeling framework. One immediate concern about cyber security threats therefore is that one single high profile event can serve as a framing event that can seem to validate many exaggerated claims, and indeed, lead to many more of such claims, which can result in over-reaction from policy-makers and the public.

Taking the lead from the psychology and social-psychology of risk literature, government should work to minimize the vulnabilities associated with perceptions of dread, lack of control and the unknown, for example; it should also contribute to alternative narratives than the ones of cyber gurus that people can imagine and from which they can learn and draw meaning for the daily lives.

To start, we must work harder to lift the veil from over cybersecurity. Reliable information related to cyber-secruity is not easily available. Neither CI owners and operators nor government readily disclose such information (Quigley 2013). Government must collect, validate and disseminate more data among owners and operators of CI to help improve our understanding of the risk.

Government officials must also encourage a more nuanced understanding of risk. 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. Moreover, government frames of reference differ at times from those of industry. 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. 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, liaibility, brand reputation, the protection of financial data and learning good 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. Relatedly, 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 and misleading.

At an institutional level, government can make progress by recognizing the importance of peer-networks for managing cyber-security risks. Each public organization should also have a highly visible and accessible "cyber-security champion" who promotes awareness of cyber-security issues but can 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. Government must also develop a more effective method to prioritize systems and the security required for such systems. We need to have a better understanding of what really needs to be protected to a high level and what does not, considering in particular the level of redundance and resilience in systems. Public bureaucracies are susceptible to regulating in the face of uncertainty (Hood 1998); over-regulating information availability jeopardizes the potential innovation and transparency of public institutions.

It is difficult to determine what influence cyber gurus actually have. Despite the 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. In one recent study they expressed concerns about risks associated with, for example, data integrity, intellectual property, privacy, reputation and the trustworthiness of security information (Quigley, Burns and Stallard 2013). Going forward, we recommend conducting a study that furthers our understanding of how IT managers monitor the external environment for emerging cyber-security threats and opportunities. It will also be important to monitor how reliable cyber gurus are over time; we can do this by examining how cyber gurus change their rhetorical strategies as more data about the viability of threats become public and the public discourse changes.

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. 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 danger. 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 roads, 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.

6.0 Works cited

Agranoff, R. (March 01, 2008). Enhancing performance through public sector networks: Mobilizing human capital in communities of practice. *Public Performance & Management Review, 31,* 3, 320-347.

Ahonen, A., & Kallio, T. (January 01, 2009). On the cultural locus of management theory industry: Perspectives from autocommunication. *Management & Organizational History, 4,* 4, 427-443.

Alhakami, A. S., & Slovic, P. (January 01, 1994). A psychological study of the inverse relationship between perceived risk and perceived benefit. *Risk Analysis, 14,* 6, 1085-1096.

Aristotle, & Kennedy, G. A. (1991). *On rhetoric: A theory of civic discourse*. New York: Oxford University Press.

Arrow, K. J. (1971). *Essays in the theory of risk bearing.* Chicago: Markham Publishing.

Attorney-General's Department. (2003). *Trusted Information Sharing Network*. Government of Australia. Retrieved from http://www.tisn.gov.au/Pages/default.aspx.

Baker, S. 2010. *Skating on stilts: Why we aren't stopping tomorrow's terrorism*. Hoover Institution Press Publication no. 591. Stanford, CA: Hoover Institution at Leland Stanford Junior University.

Berglund, J., & Werr, A. (January 01, 2000). The invincible character of management consulting rhetoric: How one blends incommensurates while keeping them apart. *Organization, 7,* 4, 633-655.

Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (July 01, 2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly, 27,* 3, 264-271.

Betsch, T., & Pohl, D. (2002). The availability heuristic: A critical examination. In P. Sedlmeier & T. Betsch (Eds.), *Etc.—Frequency processing and cognition* (pp. 109–119). Oxford: Oxford University Press.

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

Busseri, T. (March 12, 2012). It's time to take cybersecurity seriously. *Wired Magazine.* Retrieved from http://www.wired.com/2012/03/opinion-busseri-cybersecurity/.

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

Cavelty, M. D. (March 01, 2007). Cyber-terror–Looming threat or phantom menace? The framing of the US cyber-threat debate. *Journal of Information Technology & Politics, 4,* 1.

Centre for the Protection of National Infrastructure. (2006). *CPNI*. Government of the United Kingdom. Retrieved http://www.cpni.gov.uk/

Clark, T., & Salaman, G. (January 01, 1996). The management guru as organizational witchdoctor. *Organization, 3,* 1, 85-107.

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

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

Colarik, A., & Janczewski, L. (March 01, 2012). Establishing cyber warfare doctrine. *Journal of Strategic Security, 5,* 1, 31-48.

Comfort, L. (October 28, 2010). Designing resilience for communities at risk. *The CIP Initiative - Disasters in the Infrastructure: Response and Assessment Workshop Proceedings*. Retrieved from http://cip.management.dal.ca/wp-content/uploads/2013/02/cip_workshop_2010_proceedings.pdf.

Conabree, D. (2011). Intellectual capital and e-collaboration: The hidden cost of the status quo. *FMI Journal 23,* 1, 11-12.

Coughlin, C. (October14, 2010). Cyber guards or soldiers: Which do we need most? *The Daily Telegraph.*

Dearstyne, B. W. (January 01, 2005). Fighting terrorism, making war: Critical insights in the management of information and intelligence. *Government Information Quarterly, 22,* 2, 170-186.

Douglas, M., & Wildavsky, A. B. (1982). *Risk and culture: An essay on the selection of technical and environmental dangers*. Berkeley: University of California Press.

Edelman. (2013). Edelman trust barometer 2013: Annual global study: Canadian findings. *Edelman Insights*. Retrieved from: http://www.slideshare.net/EdelmanInsights/canada-results-2013-edelman-trust-barometer

Faisal, M. N., Banwet, D. K., & Shankar, R. (July 01, 2006). Supply chain risk mitigation: Modeling the enablers. *Business Process Management Journal, 12,* 4, 535-552.

Finucane, M., Slovic, P., Mertz, C. K., Flynn, J., & Satterfield, T. (July 01, 2000). Gender, race, and perceived risk: The 'white male' effect. *Health, Risk & Society, 2,* 2, 159-172.

Folkes, V. S. (March 01, 1988). Recent attribution research in consumer behavior: A review and new directions. *Journal of Consumer Research, 14,* 4, 548-565.

Fowler, T. & Quigley, K. (2014) Contextual factors that influence the Canadian government's response to the cyber threat. *International Journal of Public Administration in the Digital Age*.

Fyfe, T., & Crookall, P. (2010). *Social Media and Public Sector Policy Dilemmas.* IPAC: Toronto.

Gierlach, E., Belsher, B. E., & Beutler, L. E. (January 01, 2010). Cross-cultural differences in risk perceptions of disasters. *Risk Analysis, 30,* 10, 1539-1549.

Glenny, M. (May 18, 2011). Canada's weakling Web defenses. *The Globe and Mail.* Retrieved from http://www.theglobeandmail.com/globe-debate/canadas-weakling-web-defences/article580145/

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

Gordon, V. (October 01, 2010). National Security Directive declassification. *Government Information Quarterly, 27,* 4, 322-328.

Hansen, L., & Nissenbaum, H. (December 01, 2009). Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly, 53,* 4, 1155-1175.

Hardin, R. (2006). *Trust*. Cambridge: Polity Press.

Harknett, R. J., & Stever, J. A. (November 30, 2009). The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen. *Journal of Homeland Security and Emergency Management, 6,* 1.

Hess, C., & Ostrom, E. (2007). *Understanding knowledge as a commons: From theory to practice*. Cambridge, MA: MIT Press.

Hood, C. (1998). *The art of the state: Culture, rhetoric and public management*. Oxford: Oxford University Press.

Hood, C., & Jackson, M. W. (1991). *Administrative argument*. Aldershot, UK: Dartmouth Publishing.

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

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

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

Keulen, S., & Kroeze, R. (May 01, 2012). Understanding management gurus and historical narratives: The benefits of a historic turn in management and organization studies. *Management and Organizational History, 7,* 2, 171-189.

Kieser, A. (February 01, 1997). Rhetoric and myth in management fashion. *Organization, 4,* 1, 49-74.

Koliba, C. J., Mills, R. M., & Zia, A. (March 01, 2011). Accountability in governance networks: An assessment of public, private, and nonprofit emergency management practices following Hurricane Katrina. *Public Administration Review, 71,* 2, 210-220.

Kolluru, R., & Meredith, P. H. (December 01, 2001). Security and trust management in supply chains. *Information Management & Computer Security, 9,* 5, 233-236.

Koski, C. (January 01, 2011). Committed to protection? Partnerships in critical infrastructure protection. *Journal of Homeland Security and Emergency Management, 8,* 1.

Kramer, R. M. (January 01, 1999). Trust and distrust in organizations: emerging perspectives, enduring questions. *Annual Review of Psychology, 50,* 569-598.

Lachlan, K., & Spence, P. R. (January 01, 2010). Communicating risks: Examining hazard and outrage in multiple contexts. *Risk Analysis, 30,* 12, 1872-1886.

Langer, E. J. (January 01, 1975). The illusion of control. *Journal of Personality and Social Psychology, 32,* 2, 311-328.

Layne, K., & Lee, J. (April 01, 2001). Developing fully functional E-government: A four stage model. *Government Information Quarterly, 18,* 2, 122-136.

Lewis, J. (June 01, 2003). Cyber terror: Missing in action. *Knowledge, Technology, and Policy, 16,* 2, 34-41.

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

Maldonato, M., & Dell'Orco, S. (November 01, 2011). How to make decisions in an uncertain world: Heuristics, biases, and risk perception. *World Futures, 67,* 8, 569-577.

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

Mittu, R., Guleyupoglu, S., Johnson, A., Barlow, W., Dowdy, M., & McCarthy, S. (January 01, 2008). Unclassified information sharing and coordination in security, stabilization, transition and reconstruction efforts. *International Journal of Electronic Government Research, 4,* 1, 36-48.

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

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (June 01, 2012). SCADA security in the light of cyber-warfare. *Computers & Security, 31,* 4, 418-436.

Nørreklit, H. (August 01, 2003). The Balanced Scorecard: What is the score? A rhetorical analysis of the Balanced Scorecard. *Accounting, Organizations and Society, 28,* 6, 591-619.

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

Osborne, D., & Plastrik, P. (1997). *Banishing bureaucracy: The five strategies for reinventing government*. Reading, MA: Addison-Wesley.

Pachur, T., Hertwig, R., & Steinmann, F. (September 01, 2012). How do people judge risks: Availability heuristic, affect heuristic, or both? *Journal of Experimental Psychology: Applied, 18,* 3, 314-330.

Paquette, S., Jaeger, P. T., & Wilson, S. C. (July 01, 2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly, 27,* 3, 245-253.

Pennings, J. M. E., & Grossman, D. B. (September 01, 2008). Responding to crises and disasters: The role of risk attitudes and risk perceptions. *Disasters, 32,* 3, 434-448.

Pratt, J. W. (January 01, 1964). Risk aversion in the small and in the large. *Econometrica, 32,* 122-136.

Public Safety Canada (2009). *National Strategy for Critical Infrastructure.* Ottawa: Her Majesty the Queen in Right of Canada. Retrieved from http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ntnl-eng.pdf.

Quigley, K. (2009). Seven questions for Michael Chertoff. *The CIP Exchange, Spring 2009,* 1-2.

Quigley, K. (March 01, 2013). 'Man plans, God laughs': Canada's national strategy for protecting critical infrastructure. *Canadian Public Administration, 56,* 1, 142-164.

Quigley, K., Burns, C., & Stallard, K. (2013). Communicating effectively about cyber-security risks: Probabilities, peer networks and a longer term education program. *Public Safety Canada Contract: No. 7181309* - Identifying and Effectively Communicating Cyber-security Risks. Retrieved from http://cip.management.dal.ca/wp-content/uploads/2013/04/Quigley-Burns-Stallard-Cyber-Security-Paper-Final-1.pdf

Quigley, K., & Mills, B. (February 1, 2014). Contextual issues that influence the risk regulation regime of the transportation sector. *Kanishka Project Contribution Program - Understanding and Responding to Terrorist Threats to Critical Infrastructure*. Halifax, NS: School of Public Administration, Dalhousie University. Retrieved from http://cip.management.dal.ca/?page_id=280

Relyea, H. C. (January 01, 2004). Homeland security and information sharing: Federal policy considerations. *Government Information Quarterly, 21,* 4, 420-438.

Renn, O. (2008). White paper on risk governance: Toward an integrative framework. In O. Renn, & K. Walker (Eds.), *Global risk governance: Concept and practice using the IRGC framework.* Dordrecht: Springer.

Rid, T. (2013). *Cyber war will not take place*. New York: Oxford University Press.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (July 01, 1998). Not so different after all: A cross-discipline view of trust. *The Academy of Management Review, 23,* 3, 393-404.

Røvik, K. (January 01, 2011). From fashion to virus: An alternative theory of organizations' handling of management ideas. *Organization Studies, 32,* 5, 631-653.

Roy, J. (2012). Social Media's Democratic Paradox: Lessons from Canada. *European Journal of ePractice, 16,* 5-15.

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

Senge, P. M. (1990). *The fifth discipline: The art and practice of the learning organization*. New York: Doubleday/Currency.

Sharif, A M. (2008). Transformational government: What is the shape of things to come*? Transforming Government: People, Process and Policy, 2*, 1, 71-75.

Shore, J. J. M. (March 2008). *The legal imperative to protect critical energy infrastructure*. Ottawa, ON: Canadian Centre of Intelligence and Security Studies.

Sjöberg, L. (January 01, 2000). Factors in risk perception. *Risk Analysis, 20,* 1, 1-12.

Slovic, P. (January 01, 1987). Perception of risk. *Science, 236,* 4799, 280-5.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1979). Rating the risks. *Environment, 21*, 3, 14-20.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (June 01, 1982). Why study risk perception? *Risk Analysis, 2,* 2, 83-93.

Slovic, P., Peters, E., Finucane, M. L., & Macgregor, D. G. (January 01, 2005). Affect, risk, and decision making. *Health Psychology, 24,* 4, 35-40.

Smith, P. K., & Steffgen, G. (2013). *Cyberbullying through the new media: Findings from an international network*. London: Psychology Press.

Starr, C. (January 01, 1969). Social benefit versus technological risk. *Science (New York.), 165,* 3899, 1232-1238.

Stohl, M. (April 10, 2007). Cyber terrorism: A clear and present danger, the sum of all fears, breaking point or patriot games? *Crime, Law and Social Change, 46,* 223-238.

Strickland, L. S. (January 01, 2005). The information gulag: Rethinking openness in times of national danger. *Government Information Quarterly, 22,* 4, 546-572.

Sunstein, C. R. (January 01, 2003). Terrorism and probability neglect. *Journal of Risk and Uncertainty, 26,* 2-3, 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.

Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive Psychology*, *5*, 1, 207-233.

United States Department of Homeland Security. (2008). *One Team, One Mission, Securing Our Homeland: U.S. Department of Homeland Security Strategic Plan, Fiscal Years 2009–2013*. Washington, DC: GPO.

Vogel, D. (1986). *National Styles of Regulation: Environmental Policy in Great Britain and the United States* (Vol. 242). Ithaca, NY: Cornell University Press.

Von Solms. R., & Van Niekerk. J. (May 13, 2013). From information security to cyber security. *Computers and Security, 38,* 97-102.

Walton, D. N. (1996). *Argumentation schemes for presumptive reasoning*. Mahwah, N.J: L. Erlbaum Associates.

Wason, P. C. (July 01, 1960). On the failure to eliminate hypotheses in a conceptual task. *Quarterly Journal of Experimental Psychology, 12*, 3, 129-140.