

**Protecting National Infrastructure in the US and the UK:  
A Preliminary Examination**

Workshop 4: Transparency and Accountability in Government

Kevin Quigley, PhD

School of Public Administration

Dalhousie University

Halifax, Canada

[kevin.quigley@dal.ca](mailto:kevin.quigley@dal.ca)

Abstract:

Critical Infrastructure Protection (CIP)—activities that enhance the physical *and* cyber-security of key public and private assets—is the focus of urgent attention among Western governments in light of recent power failures, computer viruses, natural disasters, epidemics and terrorist attacks, both threatened and realized. The problems are not merely technical. Many social, organizational and jurisdictional obstacles prevent successful CIP. Drawing on the Hood, Rothstein and Baldwin risk regulation regime framework (2001), the paper will examine more systematically the CIP practices in the US and the UK. In particular, the paper examines the contextual factors, *viz.* market forces, public opinion and organized interests, which potentially influence government responses to CIP. The paper also examines processes and mechanisms each government has put in place in order to control better the security and safety of their respective national infrastructures. The paper concludes by highlighting challenges governments will have to overcome in order to gain more effective control over national infrastructure. This paper represents the early stages of a research project supported by Canada's Social Sciences and Humanities Research Council. The information in this paper is drawn largely from existing academic literature and on-line government sources.

Critical Infrastructure Protection (CIP)—activities that enhance the physical *and* cyber-security of key public and private assets—is the focus of urgent attention among Western governments in light of recent power failures, computer viruses, natural disasters, epidemics and terrorist attacks, both threatened and realized. Government studies and popular analyses note the complex, interdependent and fragile make-up of these infrastructures and the technologies that underpin them. Consider the 2003 North American power outage: overgrown trees in Ohio helped trigger a power failure that affected 50 million people and cost the US economy anywhere from \$4 to 10 billion.<sup>1</sup>

The problems are not merely technical. Many social, organizational and jurisdictional obstacles prevent successful CIP. For most Western countries, the vast majority of critical infrastructure is owned and operated by the private sector. Corporate executives and their shareholders are reluctant to spend to reduce risks associated with their critical infrastructure—particularly in poor economic times—because the benefits are often indeterminate. They are also reluctant to disclose the vulnerabilities of their key assets because of the risk to their organization’s security and share value. There is also a problem with trust. Industry executives worry that sensitive information shared with government may be used (surreptitiously) for reasons other than CIP. Government officials are equally reluctant to share sensitive information. Leaked intelligence can bring about human devastation on a massive scale. Finally, overlapping responsibilities between different levels of government can obscure accountability, complicate planning and create the conditions for bureaucratic turf wars. In short, despite its acknowledged importance, CIP is an area in which there has been little cooperation.

The US and the UK governments have taken steps to change this dynamic. Each government has created a number of mechanisms to manage critical infrastructure, including public-private sector fora whose goal is to facilitate the exchange of information about vulnerabilities. Drawing on the Hood, Rothstein and Baldwin risk

---

<sup>1</sup> US-Canada Power System Outage Task Force (2004), *Final Report*. Available at: <https://reports.energy.gov/>

regulation regime framework, the paper will examine more systematically the CIP practices in the US and the UK. The paper is organized in the following manner. First, the paper introduces the analytical framework. Second, the paper examines the contextual factors, *viz.* market forces, public opinion and organized interests, which potentially influence government responses to CIP. Third, it examines selected processes and mechanisms each government has put in place in order to control better the security and safety of their respective national infrastructures. Finally, the paper concludes by highlighting challenges governments will have to overcome in order to gain more effective control over national infrastructure.

This paper represents the early stages of a research project supported by Canada's Social Sciences and Humanities Research Council. The aim of the research project is to examine the governance of critical infrastructure in the US, the UK, Canada and Australia and consider the contextual drivers that influence the exchange of sensitive information. This paper represents a literature review of the context and management of CIP in the US and the UK. Primary data have not yet been collected.

## **I. ANALYTICAL FRAMEWORK: RISK REGULATION REGIMES**

Research in CIP is relatively new.<sup>2</sup> Important questions remain inadequately explored: What qualifies as critical infrastructure, and how is this determination made? How do elements of critical infrastructure relate to one another? Can critical infrastructure be controlled? By whom or by what? What role do social players, such as the media, civil society and interest groups, play in protecting critical infrastructure? And, for government, what tools for managing CIP are at its disposal, and in what contexts do certain tools work best?

---

<sup>2</sup> Arguably CIP dates to the beginning of modern civilization. War time frequently provides insightful examples of CIP in action. The beginning of the study of modern CIP has been identified by Brown (2006) as 1996, when President Clinton created the first presidential commission on the subject.

The number of unexplored questions can make it difficult to know where to begin a discussion on CIP. For this reason, I have found it useful in my research to adopt an analytical framework developed in 2001 in the United Kingdom by Hood, Rothstein and Baldwin. The Hood, Rothstein and Baldwin framework is designed specifically to help elucidate issues associated with risk, a key concern when thinking about CIP, and with how risk might be managed or regulated in today's context.

The Hood, Rothstein and Baldwin framework is useful for an exploratory discussion of the subject. It casts a wide net: the framework considers the law, the market, the media, public opinion, interests and institutions when examining factors that are potentially critical to understanding governments' approaches to risk management.

Hood *et al.* deploy the concept of 'regimes' to explore the variety of government responses that exist in different policy areas<sup>3</sup> (Hood *et al.*, 2001, 5). Using this diverse literature as their springboard, they define regimes thus: 'the complex of institutional geography, rules, practice and animating ideas that are associated with the regulation of a particular risk or hazard' (2001, 9). This broad definition allows for flexibility as Hood *et al.* read across various policy contexts while drawing together a variety of institutional perspectives in order to understand what shapes risk regulation.

Hood *et al.* hypothesize that within these regimes context shapes the manner in which risk is regulated, or what they refer to as 'context shapes content'. 'Regime context' refers to the backdrop of regulation. There are three elements that Hood *et al.* use to explore 'context': the technical nature of the risk; the public's and media's opinions about the risk; and the way power and influence are concentrated in organized groups in the regime. These three pressures are commonly employed explanations in the public policy literature and can be related, to some extent, to a normative theory of regulation as well as to a positive one (Hood *et al.*, 61).

---

<sup>3</sup> (1) Attacks by dangerous dogs outside the home; (2) lung cancer caused by radon gas at home; (3) and at the workplace; (4) cancer caused by benzene from vehicle exhaust; (5) and at the workplace; (6) attacks on children by paedophiles; (7) injuries and deaths from vehicles on local roads; (8) health from pesticides in food; (9) and in water (Hood *et al.*, 37).

Hood *et al.* derive three separate (but overlapping) hypotheses from these three pressures. The first hypothesis, *the Market Failure Hypothesis*, examines the government's intervention as a necessary one given the technical nature of the risk and the inability of the market to manage the risk effectively without such intervention. The second hypothesis, *the Opinion Responsive Hypothesis*, examines the extent to which risk regulation is a response to the preferences of civil society. The third hypothesis, *the Interest Group Hypothesis*, examines the role of organized groups in shaping the manner in which a risk is regulated in the industry.

Hood *et al.* use these separate hypotheses to determine the extent to which each of these aspects of context explains the size, structure and style of risk regulation, or what they call 'risk regulation content'. Regulation content refers to the policy settings, the configuration of state and other organizations directly engaged in regulating the risk, and the attitudes, beliefs and operating conventions of the regulators (Hood *et al.*, 21).

Each of the three critical elements of 'regime content' is characterized further through the three elements of a cybernetic control system—information gathering, standard setting and behaviour modification. In this sense control means the ability to keep the state of a system within some preferred subset of all its possible states. If any of the three components is absent, a system is not under control in a cybernetic sense (Hood *et al.*, 23–5). Therefore, in addition to referring to the size, structure and style of the regulatory regime, they refer to the regulatory regime's ability and willingness to gather information, set standards and modify behaviour by way of keeping the regime under control. The figure below summarises the approach.

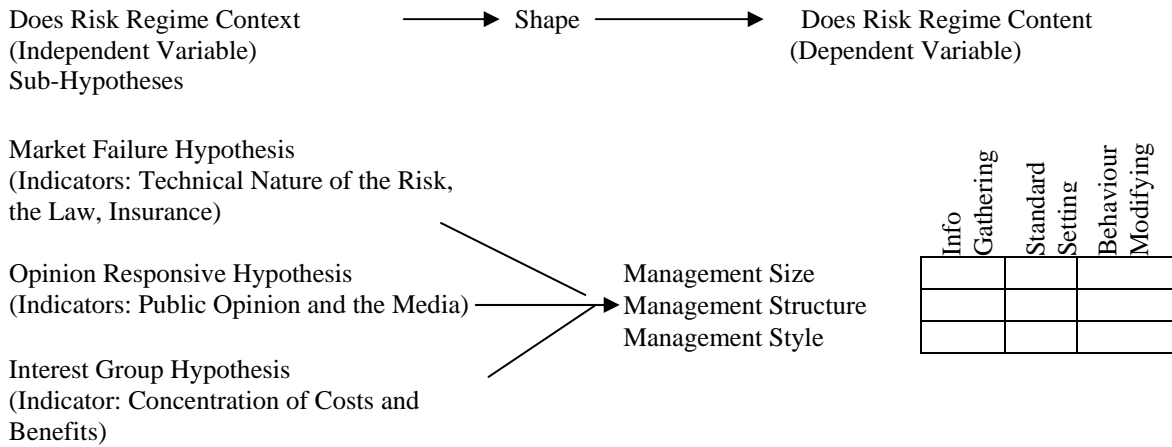


Figure 1: Risk Regulation Regime Framework

Source: Quigley (2008), based on Hood, Rothstein and Baldwin's (2001) framework

In sum, we intend, first, to explore the context that surrounds the regulation of critical infrastructure, essentially populating the left-hand side of the figure above, and second, using the Hood *et al* categories for Regime Content, to provide comments and analysis on CIP in specific countries, essentially populating the right-hand side of the above figure. The final section of the paper will examine key questions and tensions that the governments in question must confront in order to improve CIP in their respective countries.

## II. CONTEXT

### The Market Failure Hypothesis

According to the Market Failure Hypothesis (MFH), a government's approach to managing risk will reflect the inherent nature of the particular risk in question. The content of the government's regulatory regime will reflect such things as the scale of the hazards associated with the risk and the extent to which markets, and insurance markets or the law of tort in particular, are effective in regulating risk on their own.

In this section of the paper we discuss MFH in relation to risks associated with CIP. Specifically, we examine two market costs that Hood *et al.* consider key to understanding the extent to which government intervention in risk management becomes necessary: “information costs” and “opt-out costs.”

### *Opt-out Costs and Information Costs*

Opt-out costs are costs faced by individuals in reducing or eliminating their exposure to risk. Examples are costs associated with civil law processes and insurance. Information costs are costs faced by individuals in their efforts to identify and assess the level or type of risk to which they are exposed.

From an MFH perspective, Hood *et al.* hypothesize that the size of regulatory regime content is larger for high-cost cases of risk than for low-cost cases of risk. Conversely, if both information and opt-out costs are low, Hood *et al.* hypothesize that regulatory size will be smaller. If information costs are high but opt-out costs are low, market failure logic suggests regulatory size will be high for information-gathering but low for behaviour modification. If information costs are low but opt-out costs are substantial, regulatory size will be low for information-gathering but high for behaviour modification. The figure below summarizes Hood *et al.*'s expectations of an approach to regulation dictated by the logic of market failure.

Cost of obtaining information on exposure to risk			
Costs of opting-out of exposure to risk by market or contractual means		Low	High
	Low	Minimal regulation	Regime content high on regulatory size for information-gathering, with behaviour modification through information dissemination
	High	Regime content high on regulatory size for behaviour modification	Maximal regulation

*Figure 2: The Logic of a Market Failure Approach to Regulatory Size*

Source: Hood, Rothstein and Baldwin, 2001

### *The Challenges of ‘Opting Out’ in CIP*

We will look now at the role of insurance and the role of law in CIP.

#### *Insurance<sup>4</sup>*

In order to make the insurance industry viable, insurers have to be able to spread risks across a pool of policy-holders, and across time. The industry cannot, for instance, afford to make significant payouts during a concentrated period. Nor can it only insure one geographic space. The history of natural disaster insurance teaches that limited, high-risk pools may not be able to attract private insurance without subsidies (Boardman 2005).

<sup>4</sup> This section draws significantly from Boardman, M. (2005), “Known Unknowns: The Illusion of Terrorism Insurance.” *Georgetown Law Journal*. 93, 3: 783-844.

There are examples of insurance coverage in low probability/high consequence failures. These claims can be expensive. Consider the following.

<b>Event</b>	<b>Insured Loss (in millions, USD)</b>
September 11 (2001)	50 000 to 55 000
Los Angeles Riots (1992)	775
World Trade Center Bombing (1993)	510
Oklahoma City Bombing (1995)	125

*Table 2: Insurance Payouts on Low Probability / High Consequence Events*

Source: Boardman (2005)

The cost of these events can lead to protracted legal disputes over responsibility. They can also lead to the bankruptcy of the insurance (or reinsurance) sector (Boardman 2005).

Terrorist attacks differ from catastrophic natural disasters in three fundamental respects. First, natural disasters can be predicted (more reliably) using history and science, while terrorist attacks cannot be. Second, acts of terrorism are not distributed randomly across time. Events could occur in quick succession, for instance. Third, catastrophic natural disasters follow relatively random paths; a tornado might land in a field as easily as it might land in a town. Terrorists, by contrast, aim for densely populated areas and valuable property (Boardman 2005, 827). Governments will likely have had to step in to act as an insurer of last resort in acts of deliberate terror.<sup>5</sup>

Despite the capacity to predict natural disasters with more accuracy, catastrophic natural disasters still cause considerable damage that the insurance industry may not be able to cover. Insurance coverage over natural disasters have often required some government intervention. Ninety per cent of all natural disasters are floods (Boardman 2005). The primary problem for flood insurance is cost, not calculation. It is a high cost, poorly spread risk. This dynamic resulted in the creation in the US of the 1968 National Flood

---

<sup>5</sup> This creates a moral hazard problem, however. If government steps in to provide insurance individuals too readily owners will not be motivated to protect their businesses.

Insurance Program. The lesson here, Boardman concludes, is that the government can be useful in cases of the uninsurable.

There are some insurers who are known for taking on high risk, such as Lloyds of London, Munich Re, Swiss Re, and Berkshire Hathaway. Most of these organizations do not cover aspects of deliberate acts of terror. Chemical, Biological, Radiological, Nuclear Explosives (CBRNE) have traditionally been excluded from coverage in insurance policies, for instance. In any event the greater cost to the industry seems more likely to be natural disasters (Associated Press 2008).

### *The Law*<sup>6</sup>

Examining the energy sector in particular, Shore (2008) concludes that there is an inevitable legal imperative to protect critical infrastructure. He suggests changing expectations in a post 9/11 environment and insufficient counter-terrorism practices by government may lead to legal claims by perceived victims of critical infrastructure failures of inadequate duty of care.

The issue of government liability has already arisen in the U.S. The Port Authority of New York and New Jersey was successfully sued for negligent security practices following the 1993 bombing of the World Trade Center. It is not just the government that is subject to these proceedings, Shore notes. Private sector owners and operators of critical infrastructure are also vulnerable to tort law proceedings, he argues. He notes tort liability would likely occur if investments in security were not made that might have reasonably prevented or mitigated any damages. Shore suggests that government policy and strategies, industry and association emergency management and business continuity standards, and other regulatory standards provide convenient standards of care, and as

---

<sup>6</sup> This section draws significantly from Shore, J. (2008), "The Legal Imperative to Protect Critical Energy Infrastructure." Critical Energy Infrastructure Protection Policy Research Series, March, No. 2. The Canadian Centre of Intelligence and Security Studies (CCISS) at Carleton University.

such, are attractive tools for courts to use in navigating through these increasingly important issues (Shore, 2008, 15).

At the same time, the role the courts will play in CIP is still unclear. First, despite Shore's claim, risk management standards are not always clear, as security analysts have noted.<sup>7</sup> Second, legal cases can be expensive, which can act as a deterrent for those seeking legal redress.

Y2K offers an interesting example of how expectations of mass litigation do not always materialize. At one point the US Congress predicted Y2K-related lawsuits in the US would reach \$1 trillion. Ultimately, however, there were almost none. Peysner (1999) commenting on the US and UK cases explained the failure of lawsuits to materialize by noting that that pro-active, pre-event legal advice would tend to mitigate the effects in the commercial world. Peysner also noted that in the UK, in particular, there was too much risk and too few incentives for lawyers to pursue these cases, and concluded that high damages, risk free litigation, active lawyers and user-friendly procedures, conditions present in the US, for instance, but absent in the UK, must be in place before mass litigation occurs. Rather, he predicted a pressure to cooperate emerging in advance of the date-change, which is indeed what we saw (Quigley, 2008).

The US, however, does have the characteristics that Peysner notes are necessary for mass litigation and still there were few Y2K lawsuits there also. The absence of lawsuits in this case can also be attributed to the fact that when one deals with one's key suppliers, it is better to work with them collaboratively on fixing vulnerabilities than pursue them in court (Quigley 2008).

Finally, the threat of legal action can have unintended consequences that will be more difficult to capture. Some have noted, for instance, that the possibility of legal liability in the event of failure has resulted in companies refusing to accept certain contracts to work

---

<sup>7</sup> Security Analysis and Risk Management Association (SARMA) in the US notes that security standards are wanting in this field. See website for further discussion: [sarma.org](http://sarma.org)

on assets deemed to be critical infrastructure. This reluctance on the part of contractors to accept contracts in which they might share responsibility for failure could hamper the process of improving the resilience of critical infrastructure.

### *Privacy and the Law*

Various social, political, economic and technological trends have given rise to considerable debate over the concept of privacy. The relevant literature includes references to use of modern technologies and legislative tools to undermine people's right to privacy, the complexity of sharing personal data, the violations of privacy in light covert operations with respect to the *War on Terror* and the growing trend of privacy commissioners in modern democracies.

Bennett and Raab (2006) describe the conventional privacy paradigm as one that envisions privacy as an individual right. They note that this conventional paradigm has been challenged. Others interpret privacy within a broader economic, social and political process. In this latter tradition privacy is interpreted as a more instrumental or functional concept; here, privacy is seen as only one interest and one right among others, and not as an entitlement. Indeed, in this tradition, privacy is protected to the extent that it ensures (and does not undermine) important economic and administrative processes and the maintenance of public order. In this latter view, invasions of privacy are increasingly regarded as acceptable, and indeed, it is the case for privacy protection that must be argued.

Despite this trend, there have been countervailing pressures. For example, the European Convention on Human Rights in British law by the *Human Rights Act 1998* has stimulated an expectation that the case for privacy protection may be put more confidently in the jurisprudence of the coming years. The Information Commission sees this Act as making a significant contribution to the framework within which the *Data Protection Act 1998* is interpreted and applied.

In practice, Bennett and Raab argue, states and businesses are inclined to see no actual or potential inconsistency between the two approaches to privacy. They seek compromises and balance in ways that suit their interests, however benevolent they may be. Civil libertarians and privacy advocates, on the other hand, criticize the transmutation of privacy from a right to a mere functional utility that facilitates commerce or the workings of the state. The writers conclude, “Privacy regulators tend to stand uncomfortably in the middle of the road, sometimes dodging the two-way traffic, and sometimes uncomfortably switching the traffic lights to yellow in both directions” (2006 51).

### *The Challenge of Obtaining Reliable Information*

We now turn our attention to Hood *et al*'s second measure: obtaining reliable information about risk exposure. Because the systems in critical infrastructure are highly complex, interdependent and tightly coupled (i.e. with little slack) obtaining reliable information about risk exposure is often extremely difficult, if not elusive.

### *Obtaining Reliable Information in Complex Systems*

The traditional approach to dealing with complexity in systems is a reductionist one: we reduce complex systems to the operating parts, and often employ (simpler) models of these systems to understand them. This offers us a method by which to analyse and predict the failures of complex technological systems. Engineers often employ these tools, and the assumptions embedded within them. Their influence in the field of formal risk management cannot be overstated, and its capacity to provide a convincing way forward in the face of uncertainty is powerful (Jaeger *et al.*, 2001, 90).

Despite its strength, this approach to understanding risk has some important drawbacks. First, there are practical problems with obtaining data for these models. To start, the interaction between human activities and consequences is more complex and perhaps subtle than the average probabilities captured by most risk analyses. Moreover, when data is unavailable for these models—and it often is unavailable when we are exploring rare

events (for example, acts of terrorism)—the data is often estimated. Estimations embedded at several levels of complex models will undermine the overall validity of the model. Data is also often collected and models are built on past experiences, as is usually the practice in actuarial science. These models will often fail to predict new or rare events because the assumptions of the past do not necessarily hold. Second, obtaining data that reflects people's values and preferences is equally problematic. What people perceive as 'unwanted effects' or 'consequences' differ. Finally, the institutional structure of managing and controlling risks is prone to organizational failure, which may increase actual risks (Jaeger *et al.*, 2001, 86).

### *Debate about the Reliability of Complex Systems: Normal Accidents and High Reliability Organizations*

Perhaps the most popular point of reference for exploring issues of CIP within the social sciences is the debate in organization studies that is concerned with the safety and reliability of complex technological and social systems. Two schools define the field. High Reliability Organizations (HRO) theory states that hazardous technologies can be safely controlled by complex organizations if the correct design and management techniques are followed, such as strong and persuasive leadership and commitment and adherence to a 'safety culture,' including learning from mistakes, creating redundancies and increasing transparency in accountability and operational settings (La Porte, 1996; La Porte and Consolini, 1991; Weik, 1987; Weik and Sutcliffe, 2001). Normal Accidents Theory (NAT), on the other hand, holds that accidents are inevitable in organizations that have social and technical interactive complexity and little slack (i.e. tightly coupled). According to NAT, the discipline required of an HRO is unrealistic. Systems fail due to their inherent fallibility and the non-responsive nature of bureaucratic organizations. Efforts to increase accountability result in blame-shifting. Indeed, safety is only *one* priority—it competes with many others (Perrow, 1999; Sagan, 1993; Vaughan, 1996).

More recently, growing technical, social and organizational interdependencies refocused the debate from the single organization to networks of organizations. Many scholars now

consider *resilience* as the desired objective—a capacity to absorb a shock and recover to the original state. In this view, scholars accept the possibility of massive systems failures due to these complex interdependencies and advocate proactive and reactive strategies to manage a variety of possible consequences (Boin and McConnell, 2007; Clarke, 2005; McCarthy, 2007; Roux-DuFort, 2007; Schulman and Roe, 2007). Within this context, the search for security is seen as a dynamic process that balances mechanisms of control with processes of information search, exchange and feedback in a complex multi-organizational setting, which is guided by public organizations and seeks participation by private and not-for-profit organizations and informed citizenry (Aviram, 2005; Aviram and Tor, 2004; Auerswald, 2006; Comfort, 2002; de Bruijne and van Eten, 2007; Egan, 2007).

In sum, it is difficult to anticipate failures in highly complex and interdependent systems. According to the Hood et al framework, it would seem that there is a need for government involvement in managing CIP given the high costs to individuals of collecting information about the risks and of avoiding exposure to them. The need for government involvement will vary according to the nature of the risk. The need will be greater, for example, in mitigating risks from terrorism given the relative inability of the insurance industry to offer financial protection in such cases. The opportunity for individuals to recover financial losses from infrastructure failures through legal means seems to be increasing, although results are still mixed.

### **The Opinion Responsive Hypothesis**

The Opinion-Responsive Hypothesis (ORH) suggests that public attitudes shape regulatory regime content. In other words, that risk regulation is the way it is because that is how those affected by the risks want it to be (2001, 90). For this hypothesis, Hood *et al* examine the role of media and public opinion.

#### *Individual Risk Perception*

Individual risk perception is one way to understand how citizens feel about risks and offers indications about what they expect government to do in response to them. The psychometric approach to understanding risk draws on the work of cognitive psychologists such as Slovic (1992); it conceptualizes risks as personal expressions of individual fears or expectations. In this view, individuals respond to their perceptions whether or not these perceptions reflect reality.

The approach seeks to explain why individuals do not base their risk judgements on expected values, as traditional, market-motivated explanations would suggest (Jaeger *et al.*, 2001, 102–4). The approach has identified several biases in people’s ability to draw inferences. Risk perception can be influenced by properties such as perception of ‘dread’ (e.g., nuclear power and cancer), personal control (e.g., driving versus flying), familiarity (e.g., biking, skiing), equitable sharing of both benefits and risks (e.g., does everyone in the community live next to the power plant or only the socio-economically disadvantaged groups?) and the potential to blame an institution or person (e.g., the government). It can also be associated with how a person feels about something, such as a particular technology (e.g., darn computer, crashed again). People also believe that events that they have experienced personally (e.g., being assaulted) are more likely to occur than aggregate data suggest. Information that challenges perceived probabilities that are already part of a belief system will also be either ignored or downplayed (e.g., scientific report that concludes that climate change will bring about global devastation within X years will be marginalized or even dismissed by someone who has for some time not believed that climate change is a threat). Finally, there are different classes of meaning. Risk can be understood as a random threat that triggers a disaster; an invisible threat to one’s health; a balancing of gains and losses; or something to be actively explored and desired.

In short, risk decisions do not always appear immediately rational in a market-driven sense. Views can also be susceptible to fluctuations that cannot easily be explained or controlled. Risk management strategies must consider cognitive as well as emotional responses to risk.

## *Media*

Many assume the media play a significant role in how people perceive and respond to risk. The literature suggests a much more complex dynamic. Much like the risk research in general, media research on the question of risk focused originally on objectivity, rationality and accuracy of media coverage (Freudenberg *et al.*, 1996; Wilson, 2000). Researchers noted that many people base their perceptions about risk primarily on information presented in the media (Fischhoff, 1985; 1995; Kitzinger and Reilly, 1997). Yet researchers also noted the media's propensity to report the dramatic over the common but more dangerous (Soumerai *et al.*, 1992), its tendency to sensationalize (Johnson and Cavello, 1987) and its dependence on experts without having expertise itself to counteract the claims it receives from the experts (Freudenberg *et al.*, 1996). This approach loaned itself to the view that distinguishes between expertise and ignorance; it is concerned with improving communication by way of ensuring that lay mental models, for instance, correspond more closely to those of experts (Fischhoff *et al.*, 1997, as cited in Taylor-Gooby, 2004, 5).

However, more recent developments in risk research challenged this approach. On the one hand, the fundamental assumption that the media should support the public in making adequate judgements by giving objective information was challenged by the problem that often objective knowledge is unavailable (Adams, 1995; Kitzinger, 1999; Murdock *et al.*, 2003). On the other hand, the widely disseminated assumption that media reports have a determining influence on public risk perception was challenged by the observation that the 'subject' has a relatively more active role concerning the interpretation of and response to risk.

This view is not altogether new. One can see evidence of it in Downs (1972, 39–40) when he argues, for instance, that issues go through peaks and troughs of interest as people become aware of and alarmed by the 'evils' of certain issues but then either

become bored with the problem in question or realize how difficult and costly the solutions are.

More recent contributions along these lines have come, for instance, from Wahlberg and Sjoberg (2000) who note that the media's influence is too often taken for granted when in fact much of the evidence points the other way—that media are probably not a strong causal factor of (especially not personal) risk perception. Risk perception may be affected by the media but the effects are lessened by impersonal impact. Moreover, general risk perception is more easily changed than personal risk perception. Finally, it is not conclusive that risk perception changes behaviour.

Similarly, Mutz and Soss (1997) note that the media raises people's perception of the salience of a subject in the community but is much less successful in changing people's mind on a particular subject. Similarly, Atwood and Major (2000) note that people do not think of themselves as being as vulnerable to risks as others are. Indeed, some suffer from cognitive dissonance; they are unrealistically optimistic, ignoring the news and denying personal vulnerability. In other areas of research, it has been suggested that most individuals gain information from a variety of sources, not just the media (Verba and Nie, 1972), including other individuals, government organizations and advocacy groups.

Studies that compare media coverage at different points in time tend to show that the social and political context and their changes over time are essential for understanding risk reporting (Kitzinger, 1999, 59). Zinn concludes from the literature that research on the framing of risk-perception by the media can only be fully understood by simultaneous analysis of the context in which such risk-reports are embedded and a carefully constructed ethnographic analysis of the individuals' 'embeddedness' in cultural and social contexts and biographical experiences (Zinn, 2004, 16–17).

In sum, people do not necessarily seek to maximize their utility when making decisions about risk; there are a number of emotional and intellectual factors that influence their views.

Media amplifies risk issues to the public, but the media's influence is contested, and arguably often overstated. A CIP strategy rooted in this hypothesis could mirror public opinion by adopting aggressive strategies immediately following crises or high profile ('dread') risks and then reduce them over time when public opinion softens on the issue or the issue receives less attention. Relatedly, government strategies could try to persuade the public to soften its position vis a vis critical infrastructure protection. The latter may seem difficult to achieve immediately following high profile failures, however, they could be viable strategies over time.

### **The Interest Group Hypothesis**

Corporatism and Pluralism describe two different (and opposing) dynamics that potentially characterize government-industry relations. Pluralism, which suggests an open, dynamic and competitive interaction, is commonly associated with the US; Corporatism, which suggests a closed, hierarchical and disciplined one, is commonly associated with European countries, notably Germany and the United Kingdom.

Vogel's (1986) comparative description of government regulation of industry in the US and the United Kingdom might usefully be organised into three categories: style, institutional arrangements and cultural underpinnings. Vogel argues that the *style* of the US government's approach to industry is rule-driven, backed by legislation. The dynamics between government and industry are ridden with activism and conflict: resolutions and clarifications are often sought in courts. In the United Kingdom, government interactions with industry are less confrontational; they are slower and more stable, yet flexible. Unlike in the US, they tend toward the status quo, and parties are largely co-operative. Informal, off-line negotiations are common and often result in self-regulation by industry.

*Institutionally*, the US government is more fragmented and therefore provides more points of access. Industry and non-industry participants attempt to influence decision-

makers in all three branches of government. In the United Kingdom, power is concentrated in the cabinet and a strong bureaucracy. The organisations that have access to decision-making processes are invited into the circle. They tend to be larger corporations that informally represent their sectors.

*Cultural underpinnings* are more subtle but potentially have more explanatory power. While there may be respect within American society for a 'business culture,' the American public places little trust in large corporations. Americans are content to see 'big players' kept on a tight leash: government officials using legal means to challenge industry non-compliance is understood as a viable if not desirable enforcement strategy. American business people, however, are equally suspicious of government. They do not trust, nor do they particularly respect, government officials. This low-trust dynamic on all sides quickly deteriorates into excessive government demands and catch-as-catch-can behaviour from industry. In the United Kingdom, in contrast, Vogel notes that civil servants have enjoyed a comparatively privileged and respected status across broader society in general and within the private sector in particular; they are typically well connected to industry and negotiate with them frequently through informal channels. Behaviour that could be considered 'regulatory capture'<sup>8</sup> or at the very least 'conflict of interest' in the US is considered the duty of responsible Whitehall civil servants.

Vogel concludes that these approaches to regulation have different strengths and weaknesses. The US system is more competitive and dynamic: it can adapt more easily to changing attitudes and economic conditions. It can also suffer from excessive regulation. The UK, on the other hand, has a much more stable form of government-business interaction and a much more compliant business sector. The system's bias towards the status quo, however, can make it difficult for the government to introduce structural changes even when such changes are desperately needed.

There have been, of course, changes in institutional arrangements since Vogel's writing, particularly in the United Kingdom. Points of access to legislation- and regulation-

---

<sup>8</sup> A process by which regulatory agencies come to be dominated by the industries regulated.

making processes have increased. The widening reach of European parliamentary and judicial bodies, mass privatisation and agencification, to name a few, have opened-up the British civil service and challenged its cohesion and the status of its top officials.

Such an increase in decentralisation and complexity of technology and supply chains would almost certainly pose problems for Vogel's corporatist explanation for government-business relations in the United Kingdom. More suppliers and outsourcing would create more competition and conflict, and diffuse authority and specialised knowledge would make it more difficult to select a handful of organisations to represent sectors. In short, under these conditions, could a corporatist model still work in the UK?

The segmentation of suppliers arguably has decentralised authority to the point of making control over the critical infrastructure beyond anyone's grasp. The recent security threat has given impetus in both countries to call for more and better co-operation between government and owners of the critical infrastructure. Quite contrary to calls in the nineties for decentralisation and outsourcing, both the US and the UK government would like to have a closer relationship with industry in which collaborative partnerships can be formed and exploited. Perhaps not surprisingly to Vogel advocates, these calls have been met with considerable scepticism in the US in particular. Of the Department of Homeland Security's efforts to work with industry on shared CIP issues, the Government Accountability Office (GAO) has noted a trust barrier between the two that undermines effective partnerships and prevents the sharing of critical—and sensitive—information, for instance (GAO, 2001; 2004; 2005 ).

In sum, sectors have unique characteristics that will influence government's capacity to gather information, set standards and modify behaviour. Many critical infrastructure sectors are dominated by a relatively small number of organizations in the UK, in particular, which will likely make governance membership stable and cordial but difficult to influence if dramatic change is required. The legal context will make it difficult for the US government to engage directly with large industry. Moreover, while small and medium-sized enterprises (SMEs) are increasingly important in supply chains, SMEs are

difficult to integrate into governance models, particularly in the UK, and arguably the most vulnerable to failure.

### **III. CONTROL**

We now examine some of the measures the governments have put in place to manage CI. The discussion is divided along the lines of cybernetic categories: information gathering, standard setting and behaviour modification.

#### **Information Gathering**

The size of information gathering efforts in both countries is necessarily vast: they include a mix of public and private sector actors, and national, regional and local government representatives.

What is perhaps most striking structurally is each government's attempt to manage a tension noted by Normal Accidents literature years ago (Sagan 1993, for instance): decentralization is needed for managing complex systems, but centralization is needed for highly interdependent ones. With this in mind, both governments have increased the capacity for information gathering at the local level but at the same time centralized (to a degree) standard setting at the key government departments, the Department of Homeland Security (DHS) and the Home Office, respectively. Both of these departments have amalgamated a variety of disparate agencies with an eye to clarifying responsibility and authority on security while at the same time facilitating the exchange of sensitive information.

DHS has developed considerable institutional capacity to facilitate the exchange of sensitive information between and the public and private sectors. Eighteen sectors<sup>9</sup> have

---

<sup>9</sup> Agriculture and food; defense industrial base; energy; health care; national monuments and icons; banking and finance; water; chemical; commercial facilities; critical manufacturing; dams; emergency services; nuclear reactors, materials and waste; information technology; communications; postal and shipping; transportation systems; government facilities.

been identified by the DHS as Critical Infrastructure and Key Resource (CI/KR) hubs. Sector-Specific Agencies (SSAs) have been charged with the responsibility of working with stakeholders to facilitate the exchange of information.

The DHS also uses information gathering from four advisory councils,<sup>10</sup> which have a mix of public and private sector representation. These four bodies serve as external sources of information for the DHS with respect to the CIP, and provide advice on the current needs of individual sectors.

Information for the US's National Infrastructure Protection Plan is gathered through an annual reporting protocol, which includes the bodies noted above. Individual sector specific reports are amalgamated through sectoral and regional coordinating bodies to form the consolidated *National Critical Infrastructure and Key Resources (CI/KR) Protection Annual Report*, which is produced by DHS and submitted to the Executive Office of the President. The information contained within the report is used by the Executive Office to determine CIKR funding requirements (US Department of Homeland Security, 2009).

Notwithstanding the emphasis on the voluntary nature of information exchange and the importance of developing trusted partnerships, the government's style has also on occasion been much more aggressive. The US has used legal tools, for instance, to accomplish at times controversial information-gathering. The *USA Patriot Act* is perhaps the most noted piece of legislation that has an effect on information and CIP. The Act increases the ability of law enforcement agencies to search telephone, e-mail communications, medical, financial, and other records and eases restrictions on foreign intelligence gathering within the United States. Style does not end at the letter of the law, however. FBI and the Justice Department have noted in their respective audits that illegal and improper acts were carried out by US officials who used the Patriot Act to justify their actions.

---

<sup>10</sup> The Critical Infrastructure Partnership Advisory Council (CIPAC), the Homeland Security Advisory Council (HSAC), the National Infrastructure Advisory Council (NIAC) and the National Security Telecommunications Advisory Committee (NSTAC).

While the Patriot Act was used to facilitate the access to information by government officials, amendments to the Freedom of Information Act (FOIA) were used to restrict the access to information to those outside of government. A 2002 amendment to FOIA prevents the external sharing of CIKR information provided to the federal government (Whitley et al, 2007, 272). The amendments articulate consequences (e.g., fines, dismissal and imprisonment) for those found sharing sensitive information pertaining to CIP without authorization (Uhl, 2003, 277).

While the UK does not have the same degree of institutional presence as the US, we still see similar institutional trends. The Centre for the Protection of National Infrastructure (CPNI) is responsible for providing integrated security advice to the businesses and organisations which make up the national infrastructure. CPNI is an interdepartmental organisation with resources from a number of government departments and agencies. It was formed in February 2007 and – like DHS - represents the amalgamation of previously disparate entities, such as the National Infrastructure Security Co-ordination Centre (NISCC) and MI5's National Security Advice Centre (NSAC).

Locally, the UK's Civil Contingencies Act (CCA) legislates the 'cooperation' of emergency responders, which it separates into two categories. The first category consists of government agencies, local authorities and traditional emergency response groups such as fire authorities and paramedics, while the second category includes selected CI sectors that are essential to emergency response, such as utilities and transport. CCA legislation mandates information sharing among Category 1 responders only, with a view to developing emergency response plans at the local level.

The CPNI claims to maintain strong relationships with all CI players and promotes participation in 'Warning, Advice and Reporting Point' (WARP) groups. CPNI stresses the importance of commercial confidentiality among those who participate in WARP groups.

CPNI – like DHS - has considerable research and advisory services available on-line that cover security planning and asset protection, among other topics. Guidelines frequently characterize CIP practices as ‘good business sense.’ They emphasize the importance business continuity planning generally. They encourage organizations to consider security up front when planning to extend premises, for instance, noting that it will be less expensive this way.

### **Standard-Setting**

Post 9/11, many in the insurance industry threatened to stop offering terrorism insurance altogether. (In fact few insurance policies had ever covered chemical, biological, radiological or nuclear attacks.) As a result, the US government mandated the provision of terrorism insurance under the *Terrorism Risk Insurance Act* (TRIA). The Act has two separate arms: the mandatory participation arm and the compensation arm. The participation arm mandates that insurers issuing commercial property and casualty insurance offer terrorism insurance to their policyholders. The compensation arm provides money from the federal government to insurers for the payment of terrorism losses. Below a total nation-wide loss of \$5 million for a terrorist attack, insurers pay all the insured losses. Above \$5 million, insurers pay deductibles based on the premium.

TRIA was intended as a temporary measure to allow time for the insurance industry to develop its own solutions and products to insure against acts of terrorism. The Act has been renewed on two separate occasions, however, and now extends to December 31, 2014. The impact of the Act is debatable: only 10 per cent of small commercial property/casualty accounts and fewer than 20 per cent of medium-sized accounts have purchased the terrorism coverage offered to them by insurers (Boardman 823). Seemingly, the cost is too high given the level of risk to individual businesses.

In contrast, the UK has opted not to legislate terrorism insurance, though it has established a mechanism to ensure a terrorism insurance market does exist. In 2007, the

UK created the Pool Reinsurance Company Limited, or Pool Re, which is backed by the central government.<sup>11</sup>

Beyond insurance, there are a number of CIP standards that the two governments have developed. One of the central concepts is that of *All Hazards*. Both governments advocate emergency planning and CIP that prepares for any potential problems, be they person-generated or natural disasters. In fact, despite the considerable profile that potential acts of terrorism receive in government publications, the UK's *Civil Contingencies Act* (CCA) was initially a response to flooding in the winter of 2000 and the outbreak of foot and mouth disease the following year.

Most CIP activity in the UK derives from this legislation. The CCA is separated into two distinct segments. The first outlines local level emergency preparedness activities. The second segment of the CCA provides the government the authority to enact legislation enabling it to respond quickly and effectively to emergencies, regardless of the cause of the emergency.<sup>12</sup>

Structurally, the CCA separates emergency responders into two categories. 'Category 1' encompasses traditional emergency response bodies such as local police and paramedics while 'Category 2' bodies include utility firms, select transport firms and the UK's Health and Safety Executive.<sup>13</sup> While the first category is to be involved actively in emergency preparedness planning, the latter are deemed to have a 'lesser set of duties' and are meant to cooperate and share 'relevant' information with category one organizations in the context of regular 'local resilience groups' (LRG) meetings.<sup>14</sup>

---

<sup>11</sup> See for example [www.poolre.co.uk/Introduction.html](http://www.poolre.co.uk/Introduction.html)

<sup>12</sup> See for example [www.cabinetoffice.gov.uk/ukresilience/response/emergencypowers.aspx](http://www.cabinetoffice.gov.uk/ukresilience/response/emergencypowers.aspx)

<sup>13</sup> See for example [www.opsi.gov.uk/Acts/acts2004/pdf/ukpga\\_20040036\\_en.pdf](http://www.opsi.gov.uk/Acts/acts2004/pdf/ukpga_20040036_en.pdf)

<sup>14</sup> Ibid

DHS has a number of operational standards. Each CIKR hub or sector is expected to perform seven primary capabilities.<sup>15</sup> Risk analysis is also standardized to a degree; it is guided by the six factors of NIPP Risk Management Framework (RMF). The assessment of risk within this model is based on the formula of  $R = f * (C,V,T)$  in which risk is defined as a function of consequence, vulnerability, and threat (NIPP; 3.2.6., 2009).

In addition to the central information-gathering and reporting at DHS, DHS's risk management strategy is developed further at the micro-level through the use of Sector Specific Plans (SSPs), developed jointly by public and private sector. The use of SSPs is intended to facilitate effective strategies at the local level that fit effectively with the broad-based DHS mandates.

The style of how these standards are applied is difficult to describe without further research. I make the following (limited) observations. Literature would suggest there is considerable variation in the manner in which these standards are applied. There is no central regulator in local emergency planning, for instance, and therefore there will be considerable scope for implementation. 'All politics is local' as Tip O'Neill once observed, and no doubt a considerable amount of planning is negotiated locally. Equally, the sectors that make up the critical infrastructure have well developed relationships with government departments. Again, it would seem likely that standards are negotiated with the policy specific departments, which will result in considerable variation.

In the US, there are formal over-arching frameworks. The risk management strategies within the NIPP are developed to operate in conjunction with the DHS National Response Framework (NRF) and FEMA's National Incident Management System (NIMS) to provide coordinated risk coverage in the event of an incident (NIPP,3.3.1, 22). The standards set through the RMF and SSPs serve a twofold function: to both protect against unforeseen events and establish resiliency protocols following unforeseen CIP

---

<sup>15</sup> 1) Information-Sharing Governance, 2) Membership, 3) Alerts, Warnings and Notifications (AWN), 4) Suspicious Activity Reporting (SAR), 5) Document Management, 6) Incident Collaboration and Coordination (IC&C), and 7) Routing Collaboration and Coordination (RC&C) (DHS, NIPP, Information Sharing).

failures. These protocols do not necessarily provide support to implement the measures (Tutmarc; 2004, 765). Responsibility lies strictly with the organizations themselves.

### **Behaviour Modification**

There is ample evidence to suggest that both governments have changed behaviour in the area of CIP. Many information-sharing practices and standards have been put in place that did not exist before. These steps relate to behaviour modification. The 9/11 Commission reported, for example, that one of the failures of 9/11 was that the mechanisms for sharing information were not in place when the events took place. The tools and frameworks noted above go some way addressing this issue. It should be noted also that government funding for risk mitigation projects – particularly in the US - is used as an incentive to motivate behaviour change.

Second and relatedly, even if government does know of weaknesses, will it disclose the weaknesses and the recommended solutions? Intelligence agencies are not known for disclosure. And sometimes for good reasons. Indeed, industry would be less willing to share information with government if it thought government would disclose. Moreover, it is not in anyone's interests to disclose vulnerabilities to those who would do the infrastructure harm.

Third, it is difficult to prepare entirely for emergencies. Each one is unique. People respond differently to different circumstances. When the bus blew up in London on July 7, 2005, medical professionals were noted for taking to the street to help the injured. Is this because it was mandated? Unlikely. Professional training, common decency and shared humanity more likely inspired the actions. On the other hand, when a fire broke out in a Chicago nightclub, people were noted for pushing one another out of the way as they fought for their lives to gain access to one of the few exits. Perhaps more would have survived had they cooperated with each other (Clarke 2005).

One might also speculate that effective behaviour modification would require a more active and possibly intrusive government. Rather, CIP strategies frequently refer to the voluntary nature of the strategies, and of allowing sectors and businesses to adopt practices that are best suited for their own needs. Governments seem reluctant to force additional costs on businesses for low probability / high consequence failures.

In sum, both governments have spent considerable efforts on facilitating information-sharing on CIP. Both governments have also introduced legislation and created operational standards to manage CIP-related risk more effectively. The extent to which these standards have resulted in changed behaviour among key owners and operators of CI in private industry, in particular, is less clear.

#### **IV. CHALLENGES IN OBTAINING CONTROL OVER CRITICAL INFRASTRUCTURE**

This paper represents the results of the early stages of this research project. I will conclude the paper by making the following provisional observations.

The Hood *et al.* framework allows us to test the impact that various social pressures have on how governments respond to risk in the critical infrastructure. Markets, public opinion and interests – and all the sub-categories within these categories – all exert a degree of influence. While it is perhaps too early in this research to draw definitive conclusions, it is likely that no one hypothesis holds all the answers as to why governments respond the way they do. But by testing each hypothesis we come closer to understanding the issue in the round. We gain useful insights to the multiple pressures that potentially influence policy decisions about risk, each with its own merits and potential drawbacks. By conducting this research through a comparative lens, we might also draw conclusions about which pressures exert more influence in which countries.

A cybernetic understanding of control reminds us that there are three components to a control system: information-gathering, standard setting and behaviour modification. The CIP debate has focused considerable attention on the importance of exchanging sensitive information. Information exchange in the absence of standards and behaviour modification will leave the system *uncontrolled*. In some respects information-sharing is a ‘light touch’ form of regulation. The plan assumes that by sharing information, standards and behaviour modification will occur. In the absence of more transparency, this is a potential weakness, especially with respect to behaviour modification.

The information exchange issue is a two-way street. Government is expected not simply to receive information but also to provide sensitive information to owners and operators of CI. Results here have been mixed. The GAO has noted that the Department of Homeland Security is not always effective at sharing information with private sector owners and operators of critical infrastructure. This is perhaps not surprising. Leaked intelligence can bring about devastation on a massive scale. Equally important, of course, is the culture of secrecy that pervades bureaucracies – they are not designed to be outwardly accountable; this is particularly so of security agencies.

Because it is difficult to determine if organizations are actually changing their behaviour most governments refer to the notion of developing ‘trust’ among key partners: trust that people can share information in confidence; trust that people will act appropriately in protecting their critical infrastructure. Indeed, trust seems to be an important overarching theme in each government’s CIP strategy.

In fact, the governments offer little detail about what they mean when they refer to trust and how they will develop trust with owners and operators of the critical infrastructure. Many social scientists who research the subject agree that there is no standard definition for trust. There are two common approaches to understanding trust: incentive-driven and socio-cultural (Kramer 1999). With respect to the first, a model built on incentive-driven trust will work provided government’s incentives are aligned with industry interests. One can imagine instances in which they will not be. As noted in the introduction,

organizations are reluctant to disclose the vulnerabilities of their assets because of the risk to their organization's security, liability, share value and public image. Industry executives worry that sensitive information about their vulnerabilities shared with others may be used (surreptitiously) for reasons other than CIP. Insurance coverage can be expensive, and sometimes unreliable.

According to this understanding of trust, government would expend its effort on aligning private interest with public duty, akin to Bentham's duty/interest junction (Hood 1998). This would likely require more aggressive standard setting by government in CIP, with a thorough audit function to ensure that organizations are abiding by the standards. Those that were not would have to face stiff penalties.

A socio-cultural interpretation of trust also presents challenges. First, in so far as developing trust depends on cultural norms, these can be more subtle and difficult to control and nurture in a community. If possible at all (and lessons from Cultural Theory (Hood 1998), for example, and Social-Psychology suggest it will not always be possible), developing trust can take time. This reality presents opportunities and constraints for the government. On the opportunity side, much of the literature would support the government's effort to normalize relationships with industry in matters of CIP through public/private fora. On the other hand, trends that disrupt this normalization process – such as the retirement crunch that will see many staff leave the public service over the coming years – could undermine this normalization process.

Moreover, many organizations are difficult to integrate into a CIP plan. SMEs are critical to supply chains. They are also crucial service delivery agents in small towns, and because they frequently work on the smallest margins, they are least likely to have business continuity plans. Again, however, the government would have an organizational issue. One cannot invite all SMEs to a bargaining table. Nevertheless, government might wish to consider working more closely with industry associations that represent small businesses and raise awareness on the issue of business continuity among SMEs, as we have witnessed particularly in the US.

Finally, while the governments refer to ‘partnerships’ in many cases we might actually be referring to dependencies. Relationships between government and industry are not equal. Industry often has information, which can help government. But government has the option of formally regulating industry. This awareness alone prompts industry to act in ways that it would not with others on whom it depends. Equally, does government wish to be seen as a partner? It certainly has advantages, as we see in the corporatist model: stable and collegial. Government also has a regulatory (or referee’s) role to play, however. By sitting at a round table as a partner, government potentially compromises its capacity to play the role of enforcer.

## Acknowledgements

I would like to acknowledge the outstanding research support I received from two Dalhousie University graduate students, Tony Finch and Andrew Tidball. Mr. Finch conducted research on UK CIP arrangements; Mr. Tidball conducted research on the US case. In this paper I have drawn from their descriptions of each country's CIP governance arrangements. This research is supported by SSHRC Standard Operating Grant 410-2008-1357.

## Works Cited

- Adams, J. (1995), *Risk*. London: UCL.
- Associated Press (2008), "Insurers' Annual Losses on Natural Disasters Swell to \$45 B." Obtained at [www.cbc.ca](http://www.cbc.ca) on December 29.
- Atwood, L and Major, A (2000), "Optimism, Pessimism, and communication behaviour in response to an earthquake prediction." *Public Understanding of Science*. 9: 17-431.
- Aviram, A., and A. Tor (2004), "Overcoming Impediments to Information Sharing." *Alabama Law Review*, 55: 231.
- Aviram, A. (2005), "Network Responses to Network Threats: The Evolution into Private Cybersecurity Associations." *M. F. Grady & F. Parisi (Eds.), The Law and Economics of Cybersecurity*. New York: Cambridge University Press, 143-192.
- Auerswald, P. E., T. M. La Porte, and E. O Michel-Kerjan (2006), *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Cambridge: Cambridge University Press.
- Bardach, E. (1998), *Getting Agencies to Work Together: The Practice and Theory of Managerial Craftsmanship*. Washington D.C.: Brookings Institution Press.
- Bennett, C. and Raab, C. (2006), *The Governance of Privacy*. Cambridge: MIT Press.
- Boardman, M. (2005), "Known Unknowns: The Illusion of Terrorism Insurance." *Georgetown Law Journal*. 93, 3: 783-844.
- Boin, A. and A. McConnell (2007), "Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience." *Journal of Contingencies and Crisis Management*. 15: 1, 50-59.
- Brown, K. A. (2006), *Critical Path: A Brief History of Critical Infrastructure Protection in the United States*. Arlington, VA: George Mason University Press.
- Clarke, L. (2005), *Worst Cases: Terror and Catastrophe in the Popular Imagination*. Chicago: Chicago University Press.
- Comfort, L. (2002), "Rethinking Security: Organizational Fragility in Extreme Events."

- Public Administration Review*. 62: 1, 98-107.
- de Bruijne, M. and M. van Eeten (2007), "Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment." *Journal of Contingencies and Crisis Management* 15: 1, 18–29.
- Downs, A. (1972), "Up and Down with Ecology: the Issue Attention Cycle." *Public Interest*. 28/1: 38-50.
- Egan, M. J. (2007), "Anticipating Future Vulnerability: Defining Characteristics of Increasingly Critical Infrastructure-like Systems." *Journal of Contingencies and Crisis Management* 15:1, 4–17.
- Fischhoff, B. (1985) "Managing Risk Perception." *Issues in Science and Technology*. 2:3-96.
- Fischhoff, B., Bostrom, A., Jacobs, B. and Quadrel, M. (1997), *Risk Perception and Communication*. Oxford: Oxford University Press.
- Freudenberg, W.R., Coleman, C.L., Gonzales, J. and Helgeland, C. (1996), "Media coverage of hazard events: Analysing the assumptions." *Risk Analysis*. 16: 31-42.
- Government Accountability Office (2001), *Information-sharing: Practices that can benefit Critical Infrastructure Protection*. GAO-02-24. Washington DC: GAO.
- Government Accountability Office (2004), *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*. GAO-04-780. Washington DC: GAO.
- Government Accountability Office (2005), *Critical Infrastructure Protection: DHS Faces Challenges in Fulfilling Cyber Security Responsibilities*. GAO-05-434. Washington DC: GAO.
- Hood, C. (1996), "Where Extremes Meet: SPRAT versus SHARK" in Public Risk Management" in C. Hood and D. Jones (eds), *Accident and Design*. London: UCL.
- Hood, C. (1998), *The Art of the State*. Oxford: Clarendon.
- Hood, C., Rothstein, H. and Baldwin, R. (2001), *The Government of Risk: Understanding Risk Regulation Regimes*. Oxford: Oxford University Press.
- Jaeger, C., Webler, T. Rosa, E. and Renn, O. (2001), *Risk, Uncertainty and Rational Action*. London: Earthscan.
- Johnson, B. B. and Cavello, V. T. (1987), *The Social and Cultural Construction of Risk*. Dordrecht: Reidel.
- Kheifets, L., Hester, G. and Banerjee, G. (2001), "The Precautionary Principle and EMF: Implementation and Evaluation." *Journal of Risk Research*. 4(2):113-125.
- Kitzinger, J. (1999), "Researching Risk and the Media." *Health, Risk & Society*. 1,1, 55-69.

- Kitzinger J. and Reilly, J. (1997), The Rise and Fall of Risk Reporting: Media Coverage of human genetics research, false memory syndrome and Mad Cow Disease." *European Journal of Communication*. 12: 319-50.
- Kramer, R. M. "Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions." *Annual Review of Psychology*. 50: 569-598.
- La Porte, T. R. and Consolini, P. (1991), "Working in Practice but not in Theory: Theoretical Challenges of High Reliability Organizations." *Journal of Public Administration Research and Theory*. 1: 19-47.
- La Porte, T. (1996), "High Reliability Organizations: Unlikely, Demanding and At Risk." *Journal of Crisis and Contingency Management*. 4: 2, 60-71.
- McCarthy, J. A. (2007), "From Protection to Resilience: Injecting Moxie into the Infrastructure Security Continuum." Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience. *CIPP Discussion Paper Series*. George Mason University. Critical Infrastructure Protection Program. Retrieved at <http://cipp.gmu.edu/>
- Murdock, G., Petts, J. and Horlick-Jones, T. (2003), "After Amplification: Rethinking the Role of the Media in Risk Communication" in N. Pidgeon, R. Kasprson, P. Slovic (eds) *The Social Amplification of Risk*. Cambridge University Press. 156-178.
- Mutz, D. and Soss, J. (1997), "Reading Public Opinion: The Influence of News Coverage on Perceptions of Public Sentiment." *Public Opinion Quarterly*. 61: 431-451.
- Nye, J.S., Zelikow, P.D., King, D.C. (1997), *Why People Don't Trust Government*. Cambridge: Harvard University Press.
- Perrow, C. (1999), *Normal Accidents: Living with High Technologies*. Princeton: Princeton University Press.
- Peysner, J. (1999), "Y2K – Will there be a Litigation Explosion?" *The Journal of Information, Law and Technology*. Obtained on-line at [elj.warwick.ac.uk/jilt/99-2](http://elj.warwick.ac.uk/jilt/99-2).
- Quigley, K. (2008), *Responding to Crises in the Modern Infrastructure: Policy Lessons from Y2K*. Basingstoke: Palgrave MacMillan.
- Roux-Dufort, C. (2007), "Is Crisis Management (Only) a Management of Exceptions?" *Journal of Contingencies and Crisis Management*. 15: 2, 105–114.
- Sagan, S. (1993), *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*. Princeton: Princeton University Press.
- SARMA website: [sarma.org](http://sarma.org)
- Schulman, P. R. and E. Roe (2007), "Designing Infrastructures: Dilemmas of Design and the Reliability of Critical Infrastructures." *Journal of Contingencies and Crisis Management* 15: 1, 42–49.

- Sendle, E. (1998), "Auto makers battle Y2K bug in vast supplier network." *Wall Street Journal*. November 30.
- Shore, J. (2008), "The Legal Imperative to Protect Critical Energy Infrastructure." Critical Energy Infrastructure Protection Policy Research Series, March, No. 2. The Canadian Centre of Intelligence and Security Studies (CCISS) at Carleton University.
- Slovic, P. (1992), "Perception of Risk: Reflections on the Psychometric Paradigm" in S. Krimsky and D. Golding (eds) *Social Theories of Risk*. London: Praeger.
- Soumerai, S.B., Ross-Degnan, D. and Kahn, J.S. (1992), "Effects of professional and media warnings about the association between aspirin use in children and Reye's syndrome." *Millbank Quarterly*, 70: 155-82.
- Sunstein, C. (2005), *The Laws of Fear: Beyond the Precautionary Principle*. Cambridge: Cambridge University Press.
- Taylor-Gooby, P. (2006), "The Efficiency/Trust Dilemma in Public Policy Reform." *Social Contexts and Responses to Risk Network*. Working Paper 2006/9.
- Tutmarc, Elizabeth. "The War on Cyberterror: Why Australia should examine the U.S. approach to Critical Infrastructure Protection." *Pacific Rim Law & Policy Journal Association*. Vol 13, Iss 3. 2004. 743-70.
- Uhl, Kristen Elizabeth. "The Freedom of Information Act post-9/11: Balancing the public's right to know, critical infrastructure protection, and homeland security." *American University Law Review*. Vol, 53, Iss 1. 2003-2004. 261-312.
- United States Department of Homeland Security. *National Infrastructure Protection Plan*. "General Overview." 2009. Available at: [http://www.dhs.gov/xlibrary/assets/nipp\\_consolidated\\_snapshot.pdf](http://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf)
- United States Department of Homeland Security. *National Infrastructure Protection Plan*. "Information Sharing." 2009. Available at: [http://www.dhs.gov/xlibrary/assets/NIPP\\_InfoSharing.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_InfoSharing.pdf)
- US-Canada Power System Outage Task Force (2004), *Final Report*. Retrieved at: <https://reports.energy.gov/>
- Vaughan, D. (1996), *The Challenger Launch Decision: Risky Technology, Culture and Deviance at NASA*. Chicago: Chicago University Press.
- Verba, S and Nie, N (1972), *Participation in America: Political Democracy and Social Equality*. Chicago: University of Chicago Press.
- Vogel, D. (1986), *National Style of Regulation: Environmental Policy in Great Britain and the US*. Ithaca: Cornell University Press.
- Weik, K. E. (1987), "Organizational Culture as a Source of High Reliability." *California*

*Management Review*. 29(2): 112-127.

Weick, K. E. and K. M. Sutcliffe (2001), *Managing the Unexpected: Assuring High Performance in an Age of Complexity*. San Francisco: Jossey-Bass.

Whitley, Joe D., George A. Koenig and Steven E. Roberts. "Homeland Security, Law and Policy through the lens of Critical Infrastructure and Key Asset Protection." *Jurimetrics*. Vol 47, Iss 3. Spring 2007. 259-280.

Wilson, K. (2000) "Communicating Climate Change through the Media: Predictions, Politics and Perceptions of Risk" in S. Allan, B. Adam, C. Carter (eds) *Environmental Risks and the Media*. London: Routledge. 201-217.

Zinn, J. (2004) "Literature Review: Sociology and Risk" Working Paper. Social Contexts and Responses to Risk Network, University of Kent at Canterbury. Paper obtained at <http://www.kent.ac.uk/scarr/papers/papers.htm>