*Building meta-governance for strengthening critical infrastructure in Canada and in the US: The case of the "*Beyond the Border*" Initiative*

Nicolas Francoeur

Major Research Paper presented in partial fulfillment of the requirements for the degree of

Master of Arts in Public Administration

University of Ottawa
2015

Presented to Professor Eric Champagne
December 9, 2015

Abstract

This paper provides a study on the nature of trust as it relates to the theory and practice of meta-governance in the field of critical infrastructure protection. By using the *Beyond the Border* initiative as a case study, it will be argued that the primary goal of meta-governance in such an environment is to build and sustain trust in governance networks, which is achieved through an equilibrium between process design and institutional management regulatory approaches. Applying examples from the many programs and activities organized under the umbrella of *Beyond the Border*, such as the Canada-US Resiliency Experiments (CAUSE), the Canadian Critical Infrastructure Information Gateway, and others, the relationship between transaction costs and trust will be assessed. Furthermore, the significance of corporate social responsibility will be argued as an important element of trust-building in a meta-governance setting focused on critical infrastructure. The evidence shown through the *Beyond the Border* initiative demonstrates that the theory and practice of meta-governance are not so far apart and that many lessons on the links between trust, transaction costs, corporate social responsibility and meta-governance can be learned from this relatively new international development in the field of critical infrastructure protection studies.

Contents

Introduction

When faced with the task of protecting Canada's critical infrastructure (CI) and ensuring that it is resilient in the face of unforeseen disaster, knowing what role to play continues to present a challenge for government and the non-government actors who operate it. Today, our CI is interlinked quite heavily as a result of advancements in the field of information technology and cybernetics; the physical assets which we most associate with CI are controlled and connected via computer systems which exchange information over the internet. This reality presents a whole slew of new threats and vulnerabilities to CI and stakeholders are under intense pressure to ensure that their systems do not fail and endanger the assets and business continuity of other CI operators, and more importantly, the citizens who depend on the infrastructure for safety and security.

There is little consensus with regards to what "critical infrastructure" really is: academics tend to have a much broader definition of what the term encompasses compared to governments. For the purpose of this research, the working definition of CI will be inclusive of all physical assets (e.g. oil rigs, power generation stations, roads, hospitals, etc.), electronic systems that control them (e.g. specialized hardware and software), in addition to the human operators who are responsible for operating and maintaining them, such that their destruction, malfunction or absence would cause a high degree of damage in the form of lost lives, health, and safety for citizens. In Canada, it is estimated that 85% of our CI is owned and operated by private industry, making it an arms-length affair for the government to oversee. This fact, compounded by the issue that CI is now more interdependent than it ever has been and that the threats and vulnerabilities that it faces are not constrained by international borders means that we find ourselves in quite a policy "mess", so to speak. Creating a governance framework that is stable and effective enough to ensure that Canada's CI remains protected from harm and is resilient to catastrophic events seems to be a practically insurmountable task. Government has adapted to this environment by adopting a less traditional approach to governance, called meta-governance. This

means that the government is using its power to manage networks of relationships and to facilitate cooperation, and not creating policy expecting it to be implemented in traditional bureaucratic top-down fashion.

In 2011, the federal government of Canada, in partnership with the government of the United States launched an initiative called *Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness*. Under this action plan is a component dedicated entirely to critical infrastructure protection and resiliency, called the Canada-United States Action Plan for Critical Infrastructure, with it containing a plethora of additional sub-initiatives and strategies. Part of this action plan involves a series of what are called CAUSE experiments (Canada-United States Enhanced Resiliency Experiment), where realistic scenarios involving cross-border threats to critical infrastructure (e.g. hurricanes, forest fires, etc.) are tested in order to analyze the effects and to determine the optimum method of collaboration between the two countries so that resources are used as effectively as possible. There is also an information-sharing element designed through this initiative with the Canadian Critical Infrastructure Gateway and the National Cross-Sector Forum. Furthermore, the government has committed itself to investing in various CI sectors while simultaneously incentivizing its private sector owners and operators to do the same via the Canadian Safety and Security Program. The *Beyond the Border* initiative highlights how the federal government plays a critical role in coordinating efforts to protect CI, performing what can be called a 'meta-governance' function.

The arrival of such a far-reaching initiative as *Beyond the Border* raises a number of research questions. From a high level, what significance does trust play in governance networks and in what way does meta-governance play a role in building this trust? This leads to more specific research questions. First, how does a meta-governance approach such as this achieve the necessary degree of collaboration and cooperation expected from the private sector, which has its own goals and values distinct from those of the public sector? How can these CI operators be incentivized to work together and invest

appropriately in the security of their infrastructure when business values often conflict with the public sector's obligation to ensure the safety and health of society? How much should the government, acting as meta-governor, intervene in the affairs of CI businesses while still maintaining enough open space for growth and innovation to develop in the private sector CI field? To answer these questions, this paper aims to study the application of meta-governance as it is applied in the *Beyond the Border* initiative. More specifically, its goal is to explore the value of trust as it relates to meta-governance in such a tightly-knit and interdependent field as critical infrastructure protection. In order to do so, the *Beyond the Border* initiative will be used as a case study to show how importantly trust fits into the way the public sector manages to govern the complex network of relationships shared between private and other non-private actors involved in critical infrastructure resiliency and protection. It is being argued that trust serves as the basic foundation for building an effective governance network, and that the primary goal of any meta-governance strategy should be to preserve, enhance, or rebuild trust between actors so that policies related to critical infrastructure protection are formulated and implemented cohesively and effectively as a matter of public safety. Meta-governance requires balancing hard and soft regulatory approaches (referred to as institutional management and process design) in order to sustain trust in governance networks. Furthermore, insufficient levels of trust in a governance network inevitably leads to increasing transaction costs between actors, which accelerates the deterioration of productive collaboration.

This study argues that corporate social responsibility is tied to trust, transaction costs and meta-governance. When actors behave in ways that go counter to socially responsible expectations, whether out of apathy or opportunism, they contribute to the breakdown of trust in governance networks. Reduced trust then leads to elevated transaction costs, which makes relations between actors even more difficult. The reverse is also true: when actors abide by their socially responsible behaviours, trust is allowed to flourish and transaction costs are reduced, leading to healthier governance networks

overall. The *Beyond the Border* initiative serves as a current and relevant example of meta-governance at work and will be used to discuss the main argument of this paper which is that trust is the keystone to a healthy governance network and that effective meta-governance is measured by how well it can maintain that trust.

As for the methodology, the paper will be divided into three sections. The first section will comprise the theoretical concepts in order to build a framework of analysis that will be used later in conjunction with the empirical examples derived from the *Beyond the Border* initiative. This will include definitions on the concepts of governance networks, trust, and meta-governance, and will use additional ideas derived from the literature on interdependency theory (Sorensen and Torfing 2007), game theory (O'Toole 2007), and corporate social responsibility (Mauss 2007; Dandurand 2012). The second section of the paper will include a discussion on what threats, both natural and human-related, exist in the field of critical infrastructure protection, in addition to an assessment of the level of interdependency and interconnectedness that is prevalent in this area. This will serve to illustrate both the degree of danger present to modern infrastructure, and also to demonstrate what kinds of cascading effects can occur when one or more systems fail. The final section will consolidate the theoretical framework developed in the first section and combine it with the aforementioned empirical examples within the *Beyond the Border* initiative to present the argument that trust is essential to building healthy and effective governance networks, and that government acting in the role of meta-governor is tasked with nurturing that trust so that policies in the field of critical infrastructure protection are created and implemented effectively and collaboratively.

Part One: The Theory of Meta-Governance and Governance Networks

Introduction to Part One

The word “governance” is a fairly nebulous term, especially in the literature of public administration. One will not find a global consensus on its definition, but there are spheres of research that share a relatively common idea of what constitutes governance. In the study of governance networks (also sometimes referred to as policy networks), Klijn (2010: 305) defines them as "more or less stable patterns of social relationships (interactions, cognitions and rules) between mutually dependent public, semi-public and private actors that arise and build up around complex policy issues or policy programmes." This definition provides the most comprehensive description of who and what is involved in governance networks, and contrasts with more simplistic definitions that view the concept as merely referring to interactions between government actors, ignoring the critical involvement of private actors in the process.

The purpose of this section is to build up a theoretical framework for approaching the topic of critical infrastructure protection in order to understand how the *Beyond the Border* initiative makes use of governance networks to achieve its goals. As such, this part will deal strictly with the academic literature and the theories that are applied in the study of governance networks; the analysis linking it to the theme of critical infrastructure protection will be performed in Section Three.

There are many ways to approach the topic of governance networks, but this paper intends to analyze them using a particularly narrow lens. The scope here will be limited to studying the principles of governance networks using the notion of trust as the keystone for ensuring cohesive and effective policy outcomes. This approach will necessitate the incorporation of a number of additional theoretical concepts, such as interdependency theory (Sorensen and Torfing 2007b and 2007c), meta-governance

(Klijn and Koppenjan 2004; Klijn and Edelenbos 2007a; O'Toole 2007), as well as game theory and corporate social responsibility (O'Toole 2007; Mauss 2007). The goal is to look at governance networks as complex relationships involving public and private actors, and to understand how trust plays a critical role in steering these networks away from failure or stagnation. In so doing, there will be an application of interdependency theory, combined with elements of game theory, to describe these relationships as struggles based on resources and bargaining power. First, there will be definitions provided for governance networks and meta-governance respectively. Then, in order to understand how these networks can be structured, manipulated, and reorganized in a dynamic fashion for the purposes of steering them towards positive and effective outcomes using what one could call 'non-traditional' governance practices, there will be a discussion on the significance of meta-governance and its part in the literature on governance networks. Lastly, this will all tie into the significance of corporate social responsibility as it relates to maintaining trust within governance networks.

What are Governance Networks?

If we use Klijn's previously stated definition as a starting point, it is immediately apparent that governance networks involve actors from across the entire spectrum of civil society, from public actors working on behalf of the government, to private actors representing not only business, but private citizen interests as well. The concept of governance networks as we describe them stems from a relatively recent trend in the field of public administration to observe the policy process (from inception to implementation and evaluation) as a more inclusive operation, distinct from the traditional Weberian style closed-off bureaucracy. One of the first authors to truly examine this new form of governance in action was Rhodes (1997), who claims that the paradigm through which we have traditionally understood British government to function (i.e. the Westminster style of government) was no longer applicable given the changes to the role of government and the greater inclusiveness of non-government parties in the policy process. The new form of governance is one that involves

interdependent networks of government actors with a fragmentation between policy creation and implementation (Rhodes 1997). This is the result of the rise of information technology which has created a society that revolves around networks as opposed to individuals; one in which economic, social, and political issues have increased in complexity and are dealt with through networking (Castells 1996).

Thus, the study of governance networks is simply a more modern understanding of how groups of actors, from both the public and private sectors, interact together in order to achieve policy goals by aggregating their interests. To further cement the idea of governance networks, Sorensen and Torfing (2007a) provide a more prescriptive definition which builds upon Klijn's (2010). Their definition of governance networks suggests five distinct elements:

1) A relatively horizontal articulation of interdependent, but operationally autonomous actors;
2) Who interact through negotiations;
3) Which take place within a regulative, normative, cognitive and imaginary framework;
4) That is self-regulating within limits set by external agencies, and;
5) Which contributes to the production of public purpose. (Sorensen and Torfing 2007a: 9)

The first element suggests that governance networks involve a "relatively" horizontal structure of independent actors. Emphasis is being drawn on the word "relatively" because, while governance networks are invariably viewed as distinct from traditional top-down forms of hierarchical governance, there is most certainly some degree of vertical control exerted over networks in order to keep them aimed down the correct path (Klijn 2012; Klijn and Koppenjan 2004; O'Toole 2007; Klijn and Edelenbos 2007a; Peters 2010; Sorensen and Torfing 2007b). Further discussion on this idea will be provided later in this section, where the theme of trust and the importance of meta-governance with regards to process design and institutional management will come into play. The second, third, and fourth facets of

this definition, will also fall into that same discussion, as the topics of facilitating negotiations within a self-regulating normative/regulative framework fit within this narrative.

The final feature of this definition, the one involving the production of public purpose, is another way of characterizing governance networks as distinct from other groups of actors who may be working towards common goals that are not necessarily in the aim of achieving public policy goals (e.g. epistemic/scientific communities). It is important to distinguish between these two, as the theoretical implications surrounding one may not be relevant to the other. Some discussion will be added on this issue as well.

What is Meta-Governance?

Another key term that must be defined is that of meta-governance. Governance networks and meta-governance are inextricably linked to one another, and any theoretical discussions about one will implicitly involve the other. Peters (2010: 37) calls meta-governance "the governance of governance", and while this is a very simple way of putting it, it is an accurate characterization. Describing meta-governance more clearly, one could say that it is the process behind how governance networks are managed, where usually a specific group or set of actors (often referred to in the literature as "meta-governors") apply a variety of organizational management strategies to facilitate positive interactions between the various relevant parties within the network. While the aforementioned definition of governance networks provided by Klijn (2010) suggests that they are self-regulating entities, it would be false to assume that there is not normally a distinct group of players acting in the interests of coordinating exchanges within the network. Oftentimes, the literature will associate this role with that of the public sector representatives in the network (i.e. the government) (Rhodes 1997; Sorensen and Torfing 2007c; Klijn and Koppenjan 2004), but the reality is that any group of actors can assume the role of meta-governor, including private sector ones (O'Toole 2007). It merely takes a particular set of actors

who understand the aggregated interests of the other members within the network to decide to take on the meta-governor role. In this sense, meta-governance as a role and an activity is a fluid one, and may not necessarily be associated with a sole group for the duration of the network's existence.

As one would expect, there is a strong management component related to meta-governance, which can be divided in two separate categories: process design and institutional management. Both of these types of management approaches are designed in such a way as to organize a network's interests and to facilitate interactions between members that will lead to positive and useful outcomes. The key difference between the two lies in the level of hands-on intervention the meta-governor chooses to engage in in order to achieve that goal. In process design, the meta-governor is presumed to accept the various features and characteristics that are already intrinsic to the network (i.e. traditions, rules, values, etc.), and is merely seeking to promote cooperation between actors so as to achieve a desirable outcome (Klijn and Edelenbos 2007a). Policy networks tend to operate under a "policy paradigm" which consists of the framework of values and ideas for discussing policy among relevant actors and which limits the boundaries on what can be argued acceptably and what cannot. The paradigm itself is rarely up for discussion and is difficult to change (Hall 1993). A meta-governor who chooses to play by the rules of the existing network without attempting to reshape them is considered to be engaging in process design; they are merely facilitating open discussions and guiding the deliberative process towards a particular outcome.

On the other side of the coin is institutional management, which requires the meta-governor to intervene more directly in the governance network in order to restructure it. In some cases, a network may become so stagnant that it fails to produce innovative solutions to policy problems, or could even become so entrenched in internal conflicts over values and goals that no consensus is ever reached on an issue (Sorensen and Torfing 2007b). In these instances, a more interventionist role is required of the meta-governor, who will have to resort to using its resources (legal, financial, and/or institutional) to

reorganize the network in such a way that it becomes productive again (Sorensen and Torfing 2007c). Interventionist strategies in this category can range from demanding reporting requirements on performance, offering financial incentives to redistribute resources to specific actors, even going so far as deciding who has a seat at the table within the network (i.e. controlling membership) can greatly impact how decisions will be made in the future (O'Toole 2007; Schattschneider 1960). As such, process design and institutional management serve as a sort of toolkit for meta-governors who have a full spectrum of strategies for managing governance networks, from soft steering mechanisms to more coercive, interventionist approaches (Kickert et al. 1997; Rhodes 1997).

Trust in Governance Networks: Balancing Conflict and Consensus

The previous discussion's focus on meta-governance covered the function of meta-governors and tools available to these actors when handling aspects of governance networks. Until now, however, the discourse has omitted the critical nature of trust in the ongoing operation of governance networks. Trust goes beyond basic rules or laws which can help mitigate opportunistic behaviours by actors. It is an ongoing activity which has powerful effects on how actors within networks interact. It helps to break uncertainty because trust in an actor allows for conscious decisions to be made where the assumption is that the other actor(s) will not behave opportunistically (Klijn and Edelenbos 2007b). A succinct definition of trust describes it as "the actors' more or less stable, positive perception of the intentions of other actors, that is, the perception that other actors will refrain from opportunistic behavior" (Klijn 2010: 310). This then begs the question: how does a governance network instill a sense of trust among its members? The answer to this question is found in the practice of meta-governance.

The tools used in meta-governance (i.e. process design and institutional management), are what are used to create an environment where actors can trust one another and work collaboratively. As it was mentioned earlier, which tool to use depends on the current state of the governance network and

what needs to be accomplished. Some networks suffer from too much conflict over even the most basic of issues, to the point where little to no progress is ever made from a policy-making perspective. Other groups sometimes face the opposite problem; they are so concerned about running into confrontation over ideas that they merely accept piecemeal, incremental solutions in what Charles Lindblom (1959) famously called the science of "muddling through". While these are two distinct types of problems faced by governance networks, they share the common symptom which is a lack of trust.

It is essential to strike a balance between consensus and conflict within governance networks in order to ensure that they are healthy and producing innovative results. Some of the literature on this topic tends to focus too much on the aspect of conflict causing networks to fail (Sorensen and Torfing 2007b and 2007c; Schaap 2007), failing to consider the possibility for networks to degrade into a state of stagnancy as a result of too little conflict. We often see governance networks as consensus-building activities where consensus is always something to strive for. This has been critiqued by others (Brans 1997; Koppenjan 2007) as a limited viewpoint on the subject and it has been argued that too much consensus can be unhealthy for these networks. It is said that striving too much for consensus can "lead […] to protracted deliberation processes that consume excessive energy and money but ultimately produce weak compromises, deadlocked decision making or non-implementation" (Koppenjan 2007: 134). Consensus at the institutional level sets the framework of rules and values for how actors interact with each other, whereas conflict ensure that these rules and values are sometimes challenged and new ideas are brought to the table in order to avoid creating an echo chamber effect (Koppenjan 2007).

Governance networks can be looked at using interdependency theory, which suggests that they are "an interorganizational medium for interest mediation between interdependent, but conflicting actors each of whom has a rule and resource base of their own" (Sorensen and Torfing 2007a: 18). From this perspective, it can be inferred that interdependency theory draws from various aspects of rational choice theory and game theory, as well as having strong ties to Crozier and Friedberg's (1980) notion of

"strategic analysis". All of these have the common attribute which views actors as behaving in such a way as to optimize their individual interests, using whatever resources and information they have at their disposal to make the most informed decision. Thus, governance networks are the result of actors using and exchanging their resources to bargain in favour of their interests, and the complex interactions that result from this dynamic leads to instances of conflict and consensus where eventually a decision must be reached.

Crozier and Friedberg (1980) developed the concept of the strategic actor, and they argue that conflict between actors can lead to new angles being presented on a problem. Conflicts are usually the result of an asymmetrical balance of resources amongst actors. The primary resource held by actors in governance networks is information, such as expert knowledge or privileged information about a given subject. Actors in possession of such information are unlikely to voluntarily share it unless there is a foreseeable benefit to them as a result of that interaction. This is where trust plays a critical part in ensuring the free flow of information between members in a network; the assumption is that the recipients of said information will not resort to opportunism and betray the trust of the actor sharing it. Selsky and Parker (2005) refer to a social construct called a "resource dependence platform", which is a view suggesting that organizations will only attempt to collaborate due to their lack of expertise in certain areas and due to a greater level of environmental uncertainty. We see this thought also in the work of Haas (2004), who argues that epistemic communities (i.e. non-government communities of subject matter experts) should remain isolated from the bureaucratic and politicized influence of government because it could have a corrupting effect on the types of solutions that are devised to solve a problem. However, the literature on meta-governance would strongly caution readers against this absolutist point of view, as it negates the value of trust in the management of networks. There is a deeply rooted belief in the field of public administration that government and epistemic communities should have an interactive relationship, and that each group has its part to play in ensuring that the

policy process operates smoothly. There is no doubt that some degree of separation between the meta-governor and the other group members in a network is necessary, but it is best to think of the separation as a type of sliding scale that shifts based on the level hands-on meta-governance required to keep a network organized (Peters 2010). Epistemic communities are not immune to the effects of perpetual conflict or intellectual stagnancy that hinder the development of creative solutions. Trust is not inherently found in networks, and in order to build it, the network needs to be properly managed in such a way that interactions are facilitated between actors (Klijn 2010). Therefore, it is the role of the meta-governor to intervene as it sees fit. A functional network with a reasonable amount of conflict and consensus may only require a process design approach where "soft" steering mechanisms are used to direct the focus of actors and to encourage resource sharing where it might be lacking. This presumes that there is already a certain degree of trust in the network and that information is still able to flow relatively efficiently. However, a disorganized network prone to breakdown in communication and collaboration may necessitate more direct intervention – an institutional management approach – where the rules and values that hold the group together could be restructured, even going so far as opening or closing off membership of the group to certain actors. This is the type of situation where trust is blatantly absent from the network and its members and the application of soft steering techniques will not be sufficient to restore network productivity. Meta-governance is thus a balancing act between coordinating networks and actors to achieve policy goals while also trying to maintain the autonomy of those actors in the network (Peters 2010). Having the right balance of conflict and consensus in a network is critical to its health and trust is vital to the harmonization of group behaviour.

Network Failure: Trust and Transaction Costs

Another factor that can lead to network failure and which is also tied to trust is high transaction costs. When referring to transaction costs, it is the amount of energy and/or resources (financial or otherwise) that an organization must output in order to bargain with another. Under interdependency

theory, one of the main objectives of meta-governance is to minimize transaction costs so as not to restrict the development of shared goals (Sorensen and Torfing 2007c). A number of things can contribute to elevating transaction costs, such as too much conflict within a network, inadequate levels of communication, or a lack of coordination of efforts, all of which can be attributed to a deficiency of trust. The simple reality is that one of the major benefits of trust is that it helps to reduce transaction costs for cooperation (Klijn and Edelenbos 2007a).

With that said, the best way to maintain lower transaction costs in a governance network is to have effective meta-governance to shape and steer the network so that it avoids the aforementioned pitfalls. It is argued by Farneti et al (2010) that the more complex relationships between actors require an even more sophisticated (and therefore costly) governance model to accommodate them. What this means is that in complex network governance arrangements where many actors and resources are at play, the input costs for bargaining and maintaining the overall health of the network are greatly increased. Thus, actors will spend more time and resources simply interacting with one another, and the meta-governor will spend a significant amount of energy in coordinating the network. In simpler arrangements, where fewer actors are present and the primary method of control in the group is contractual in nature (i.e. bound by legal agreements, with clearly defined penalties for improper behaviour) transaction costs are normally not very elevated. Considine (2003) refers to this as a "market governance" rationality, which is best suited to relatively simple partnerships, but which relies more heavily on coercive modes of control in the form of legally-binding contracts. One can therefore imagine that the very complex nature of governance networks, which can include any number of formal and informal partnerships between various public and private actors would be ill-suited to rely purely on a coercive contractual "market governance" framework. Because of the fine balance the meta-governor must account for in its application of process design (soft) and institutional management (hard) methods

of control, meta-governance stands in a category of its own when it comes to models of governance (Considine 2003).

The cost of cooperation in governance networks, by their very nature, is quite high. If a meta-governor wanted to exert complete control over the network in order to ensure full compliance and cooperation, transaction costs would skyrocket as a result of the need to create and manage many contracts between the many parties involved in the network (Williamson 1996). It would quickly become unmanageable and the network would instead degrade into a state of inactivity. This is where the importance of trust becomes apparent; trust can be harnessed as an alternative means to relying on contracts and other more coercive measures of control (Nooteboom 2002; Klijn and Edelenbos 2007b).

Game theory can be used to visualize how transaction costs are affected by trust as a variable. The Prisoners' Dilemma is often cited in the literature as a simulation of interactions in governance networks. If, for example, a group of actors is unwilling to collaborate due to high levels of uncertainty with regards to the intentions of the other parties in the network, then they may resort to "defensive, non-cooperative strategies" (Sorensen and Torfing 2007b: 100). O'Toole (2007: 223) refers to these as situations of "mutual defection" which can lead to a case where the solution for both parties that result from their interactions (or lack thereof) is far from optimal. Trust, then, is indisputably essential to the coproduction of positive outcomes in governance networks, especially when viewed from a Prisoners' Dilemma scenario. If both parties can operate under the assumption that the information or resources they have will be used appropriately, then the resulting benefits will be shared by all. This leaves no incentives for defensive strategies that sully the spirit of collaboration and cooperation. It is therefore crucial in the practice of meta-governance to ensure that the atmosphere in the network is conducive to trust, which means a careful balance of process design and institutional management is required.

Finally, the notions of trust, transaction costs, and meta-governance can be linked to corporate social responsibility (CSR). When referring to CSR, it is describing the expected level of social-mindedness that aims to deter socially irresponsible behaviour from corporations in the aim of profit. Because governance networks are composed of a plurality of private and public actors, there is a certain expectation that meta-governance has a built-in role at fostering a greater sense of CSR. As mentioned previously, relying solely on coercive measures to seek compliance is unsustainable in a governance network arrangement. Therefore, it is again the responsibility of the meta-governor to strike the balance between process design and institutional management strategies of network control in order to build an environment favourable to positive CSR behaviour. Tying this to trust and transaction costs is rather simple. CSR can be related to Mauss's (2007) notion of "the gift", which suggests that there is a triple-obligation effect driven by society when one party is given something which benefits them (a "gift"). The argument goes that society grants private entities the ability to conduct their operations using the resources that the community has allowed it in order to prosper. The implication behind this is that, once the gift is received, there is a subsequent obligation for the receiver to accept it and to repay it in the future. Translating this to CSR, this means that the private sector must express its gratitude and repay its gift in the form of socially responsible behaviour that benefits everyone. Thus, CSR is truly driven by social pressures and not merely an abidance to certain laws (Dandurand 2012). Linking this idea to trust and transaction costs, it can be safely argued that if certain actors in a network do not fulfill their CSR obligations, trust across the group will diminish (other actors will see this as a sign of opportunistic behaviour and society will be less likely to entrust other private actors with their "gifts"), and consequently, transaction costs will rise as well. This can have a cyclical effect where trust is reduced and transaction costs become so high that there remains practically no incentive for actors to uphold their CSR obligations. The importance of this will be discussed at length in the final section of this paper as it will be related to critical infrastructure resiliency. For now, this merely demonstrates the

importance of effective meta-governance as a means of avoiding a breakdown of trust that can result when negative CSR behaviours are not kept in check.

Summary

This section focuses on the clarification of two complex notions: governance networks and meta-governance. Given the degree of complexity in terms of the relationships present in governance networks, meta-governance and its range of tools and strategies including process design and institutional management is the most effective way to coordinate these relationships in order to ensure that the outcomes they produce are positive and productive. In this study, we argue that the main ingredient binding all of this together is trust, which takes quite some time to build and very little time to break. When the trust is lost as a result of ineffective meta-governance, transaction costs are elevated, leading to more caustic relationships and fewer positive policy outcomes and solutions. Corporate social responsibility also fits into this, because the involvement of public and private actors contributing to common policy goals requires socially responsible behaviour. Failure to meta-govern an environment conducive to positive CSR behaviour can result in the breakdown of trust in the network, leading to greater transaction costs, and so on. The following section of this paper will shed some light on the current threats to critical infrastructure in the modern era, while also providing a description of the level of interconnectedness and interdependency that is found in this area.

Part Two: Vulnerabilities and Interdependencies in Critical Infrastructure

Introduction to Part Two

When considering the risks linked to critical infrastructure, the average person will typically think of large-scale natural disasters or even devastating terrorist attacks. Major events in recent memory such as 9/11 and the 2011 tsunami in Japan drew considerable attention from the media and the public is left feeling justifiably concerned about future reoccurrences of these types of incidents. The reality is that there are many other types of threats and vulnerabilities associated with CI that do not make the headlines; they remain pervasive yet are obscured by their lack of sensationalist consequences. Some of these lesser-publicized threats include cyber attacks, industrial espionage and sabotage, and simply even natural degradation of physical infrastructure. However, one of the most dangerous vulnerabilities to critical infrastructure today which is rarely considered by the population or the media is the effects of interdependencies and the potential for cascading failures of critical systems across multiple sectors. Much of the day-to-day operations of most CI sectors in North America rely intrinsically on support from other sectors. For instance, the energy sector depends upon the telecommunications grid for its remotely-controlled monitoring and operations, and the transportation sector hinges directly on the energy sector (specifically oil and gas) to fuel its activities. The failure of one can and often will lead to the failure of another down the line.

This section is designed to elaborate on the types of threats and vulnerabilities faced by CI operators in North America, in addition to a description of the current environment of interdependency and shared risks among these actors. This will provide the necessary context for a subsequent analysis of the *Beyond the Border* initiative which addresses, as a part of its mandate, the risky nature of CI operations and how best to coordinate efforts beyond national jurisdictions. One part of this section will be dedicated solely to highlighting the threats and vulnerabilities present today and some of the

strategies used to combat them. Following that, a separate discussion on the nature of interdependency across CI sectors and beyond jurisdictional boundaries will be provided, thus setting the “landscape” for CI protection and resiliency.

Threats and Vulnerabilities to CI

While the average citizen certainly has a basic idea about what critical infrastructure is about, it is still helpful to provide a definition of what it is from the perspective of government. Public Safety Canada defines critical infrastructure as:

> [the] processes, systems, facilities, technologies, networks, assets and services essential to health, safety, security or economic well-being of Canadians and the effective functioning of government... Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence. (Public Safety Canada 2010)

In order to begin illustrating the various types of threats prevalent to the world of CI, it is important to first provide an account of the economic and regulatory framework within which it resides. One of the most significant facts to remember is that the vast majority of CI is owned and operated by the private sector, with estimates suggesting over 80% of said infrastructure is being run by private entities (Gendron 2010; Baker et al. 2010; Robinson et al. 1998). This arrangement, by its very nature, is conducive to a lesser degree of regulation and oversight to the benefit of efficiency and lower costs - a staple of the New Public Management system of beliefs. Public enterprises have generally fallen by the wayside in favour of greater privatization because of the perceived benefits derived from lower costs and improved services as a result of competition (Bernier and Simard 2005), and with this reality comes a particular set of risks. In the realm of CI, the concept of "risk" is a combination of threat, vulnerability, and consequence (OCIPEP 2003). The level of risk for CI will differ depending on which sector it is in and to what degree various countermeasures have been developed to mitigate it. Such countermeasures

can range from the obvious physical security, to internal company practices, as well as government and self-regulation as a motivating force for reducing risk.

There is such a broad range of threats, however, making it almost impossible to adequately protect infrastructure against all of them. The types of threats can be categorized into three groups: natural hazards, accidental threats, and malicious threats (OCIPEP 2003). Each of these threat types will now be discussed and examples will be provided to illustrate the challenges and dangers faced by CI operators.

Natural Hazards

Natural hazards, are distinct from the other types of threats due to the fact that they do not involve a direct human element as the cause. While there is certainly an indirect effect humans have on the potency of natural disasters, this effect is limited to such conditions as lack of preparation or foolish reactions to the event, thus amplifying the damage done. Obvious recurring examples of natural disasters include hurricanes, floods, earthquakes, and forest fires. These events can range in the scale of their destructive power, but suffice it to say that the damages caused by these forces of nature have been, and will continue to be, extremely costly in terms of human life, physical assets (i.e. critical infrastructure), and in relief funds. In fact, it has been argued that the greatest threat to CI in Canada is natural hazards, magnified by increasing system degradation (Graham 2013). This claim is supported by ample evidence, with figures showing that the monetary costs of natural hazards vastly outweigh those caused by humans (Auerswald et al. 2006). The huge disparity in terms of costs as a result of natural disasters, especially over the last 25 years is argued to be in part because private sector entities are continuously seeking to cut costs where possible in order to maintain their critical competitive edge, and also due to economies of scale causing the effects of natural disasters to reach greater numbers of people (e.g. as cities grow denser, the infrastructure supporting that growth is stretched to the limits of

its capacity) (Auerswald et al. 2006). Natural disasters, big and small, continuously test the resiliency and robustness of CI all around the world. Because CI operators cannot control when events such as these occur, their success is measured based on how well their infrastructure is protected, in the sense that operations are relatively unhindered after an event (i.e. a *robust* system), in addition to their ability to rapidly "bounce back" from a system failure (i.e. a *resilient* system).

Accidental Threats

As the word implies, there are threats to CI which are the result of accidents. However, these are not to be confused with natural hazards. Accidental threats are the result of human-engineered problems which manifest themselves in unforeseen circumstances. Examples of these would include failures of mechanical equipment (e.g. a turbine in a hydroelectric dam breaks), and computer-related failures - programming errors in system code, for instance. Much like natural hazards, accidental threats are not events that CI operators can properly anticipate, but they can still design their systems and processes to account for the possibility of a failure as a result of human-related accidents. In reality, accidental threats to CI are arguably the least likely form of hazard to occur today. The reasoning for this is that there is immense pressure on CI operators to ensure that accidents do not cause any dramatic system failures for a variety of reasons, including company image and business continuity. Thus, these operators tend to invest more heavily in redundancies to their infrastructure (OCIPEP 2003). Furthermore, accidental threats will continue to become less frequent as, unlike natural disasters, an operator can identify its vulnerabilities caused by accidents and address them through continuously evolving business practices.

Malicious Threats

Critical infrastructure, by its very nature, is often the target of attack from parties who would wish to harm those who depend on it, whether it is to make a political or ideological statement (Likar

2011), for hurting competition, or to benefit financially from stolen information. Regardless of the reasons for an attack, malicious threats to CI have come to be heavily represented in modern media despite the fact that, as mentioned above, their occurrences are dwarfed by the impact of natural hazards. The most interesting feature of malicious threats is that they add an entirely new dimension of vulnerabilities to CI: cyber security. Whereas natural and accidental threats primarily pose dangers to the physical assets of CI, malicious threats can target both; in fact, cyber threats have become even more commonplace due to the significant reliance on electronic systems to manage the day-to-day operations of infrastructure. Since 9/11, mainstream media has undeniably focused heavily on the physical threats to CI by presenting stories of public transportation bombings, attacks on oil and gas pipelines, and more. This is mainly because stories portraying physical destruction tend to be more sensational and are more easily understood by the general population compared to the "invisible" threat of cyber attacks.

Statistics from the Global Terrorism Database, a repository of information on all forms of terrorist events since over several decades, indicate that less than 7% of terrorist attacks globally from 1970 to 2012 fall under the category of physical facility/infrastructure attacks (Lafree et al. 2015). Further studies providing a risk assessment for the types of threats to energy infrastructure in Canada suggest that terrorism and environmental extremism (eco-terrorism) rate in the range of *very low* to *low* (Benoit 2011). In essence, the physical threat to infrastructure caused by terrorism is greatly exaggerated compared to the more prevalent and sinister threat from cyber criminals.

Cyber threats to CI can be perpetrated by foreign entities or by insiders, such as employees and consultants. External threats consist mainly of unauthorized access to computer systems to obtain or manipulate sensitive information (commonly referred to as hacking). Spear-phishing and SQL injections are among the most common types of hacks, but social engineering (manipulating interpersonal relationships to gain access to restricted information) is another form of malicious cyber attack (McAfee

2011). Insider threats, on the other hand, are defined as "individuals with access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm" (Noonan and Archuleta 2008: 11). Economic espionage is a great concern for CI operators as it can be committed by both foreign entities and insiders. State-sponsored hacking for corporate espionage is a very common occurrence (Rudner 2008; Shakarian et al. 2013). It is estimated that economic espionage costs Canada somewhere in the range of $10 to $12 billion every year (Pierrebourg and Juneau-Katsuya 2009); this is primarily in the form of lost contracts, diminished market share and reduced competitive advantage (CSIS 1995).While these issues do not appear to be immediately threatening to the ongoing operation of CI, the persistent threat of cyber crime forces operators to invest substantial resources in fending off these types of attacks on a regular basis - resources that could be better invested in a more robust and resilient infrastructure. Still, cyber attacks can result in more than just economic problems, but can also result in complete system shutdowns, due to the heavy reliance on interconnected computer systems to monitor and execute processes. Clarke (2010) claims that our dependency on information technology could bring down a number of major CI systems in less than 15 minutes as a result of a well-concerted attack. For these reasons, cyber threats are looked at with increasing attention from private and public sector actors alike.

The interdependency of CI: How connected are we?

We live in an era where CI resiliency cannot be understood by simply looking at it sector-by-sector; impacts to the continuity of operations of one sector can have dramatic cascading effects on seemingly unrelated CI sectors. For instance, when the telecommunications infrastructure suffers from a large-scale failure as a result of an attack, an accident, or a natural disaster, the water treatment plants, which rely on remotely-controlled supervisory control and data acquisition (SCADA) systems, may also fail in consequence. As mentioned previously, the prolific use of interconnected electronic control

systems has made CI as a whole more vulnerable in the face of all hazard types. Several subject matter experts argue that due to the highly complex webs of interdependent infrastructures we currently have, there is a veritable "domino-effect" that could take place given the appropriate circumstances, leading to cascading failures of multiple CI sectors (Robinson et al. 1998; Lagadec 2006 et al.; Lagadec 2009).In the CI community, dramatic cascading failures caused by a highly improbable, unpredictable event is referred to as a "black swan" (Taleb 2007). On the other hand, there is research which suggests that the common perception of CI failing in domino-style is a misconception. Van Eeten et al (2011) have argued that cascading failures tend originate from the same two sectors: energy and telecommunications (47% and 44% respectively). Their logic holds up, as it is difficult to imagine a scenario where a sudden failure in the healthcare sector causes a subsequent failure in the energy sector. What the energy and telecommunications sectors have in common is a significant dependence on electronic controls which automate many of their ongoing functions.

Cyber security has thus become a hot topic issue for private and public sector CI stakeholders, because so much depends on a network of electronic systems which contain critical information about CI technology and practices, and which also provide the backbone for routine operations. CI operators continue to invest greater amounts of their resources into fortifying their cyber front line, but the rationale behind these investments may not always be born of a sense of altruism or regard for the well-being of society at large. Private and public sector CI operators tend put greater emphasis on very different types of threats. One will find that private sector CI owners are more concerned with aging infrastructure and unintended failures, whereas public sector officials more often emphasize terrorism and deliberate attacks. Graham (2013) claims that this is because both parties seek to preserve their reputation; those in the private sector will face significant negative public relations as a result of failures from environmental damage, while government will have to deal with the political fallout of terrorist attacks. In fact, a survey of private CI operators indicated that, aside from the monetary costs, the

greatest fear for companies is damage to their reputation (Baker et al. 2010). This argument is interesting because it identifies a dynamic in the way different threat types are perceived as falling under the purview of either private or public actors.

Trust and Regulation: Striking the Delicate Balance

This then begs the question: who does what? Or more specifically: which facets of CI protection are the responsibility of the public sector as opposed to the private sector? One of the side-effects of having the private sector hold a majority stake in the ownership of CI is that it can oftentimes be difficult to reconcile their business-oriented priorities with those of the public sector, namely highly secure infrastructure with as little potential for social disruptions as possible (De Bruijne and Van Eeten 2007). More often than not, private sector businesses create their organizational processes by focusing on business continuity and will consider cascading failures (a high consequence, low probability threat) as irrelevant and out of scope (Van Eeten 2011). There are simply not enough incentives for risk mitigation when one actor's security is dependent on the security of others. If a company only has to worry about its own security without concern about it affecting others downstream, the risk analysis is far easier and therefore makes it more likely for the company to invest properly in security measures. When dependencies enter the mix and complicate the risk analysis, companies will forego investing in security and attempt to pass off the responsibility to their dependent counterparts (Kunreuther and Heal 2003; Heal et al. 2006). The net result is a greater degree of risk and a lack of security across multiple CI sectors.

This is where the public sector can fill in the gaps. One of the most vital components to building a network of secure, interdependent CI sectors is to have open information sharing between relevant stakeholders. Regardless of which type of threat is being dealt with, mutual sharing of information can help CI operators to respond more effectively to dangers and reduce their security costs overall. When

discussing CI, Branscomb and Michel-Kerjan (2006) identify two types of information: *operational* (what private entities possess, i.e. prevention, mitigation, and recovery operations) and *intelligence* (information on risks and potential consequences, often in the hands of government officials). Combined, operational and intelligence information shared amongst relevant actors can build a greater collective consciousness about the vulnerabilities to CI. Despite the benefits to sharing these types of information between private and public sector actors, there is still a "cultural reluctance to share information" in the field of CI (Graham 2013: 22). Issues of confidential business data and classified government documents create situations where potential recipients of shared information are not trusted, whether for legal or competitive reasons (Baker et al. 2010). Public sector entities will fight over jurisdictional boundaries and constitutional responsibilities, while private sector companies will hold their proprietary information close to heart.

In the absence of trust, regulation can help to address many of the shortcomings with regards to CI resiliency. There are two ways to conceive of regulation: inter-sectoral self-regulation as well as third-party intervention (i.e. government imposed sanctions). Each of these can be used appropriately in the right context in order to improve the greater landscape of CI resiliency. The literature on this subject suggests that trade associations are a method of fostering an environment of self-regulation among private sector CI operators (Hay 2006; Heal et al. 2006). These trade associations are voluntary bodies that mutually enforce abidance to various security protocols and standards; a company seen as not belonging to a well-reputed trade association may be shunned by the community, which could be detrimental to business. While this concept appears simple and effective, it does not account for the effect of "contamination". There is an alternate argument proposed whereby interdependent firms are considered to have fewer incentives to invest in security if other related firms have not (Heal et al. 2006). The logic behind this is that, if one or more entities who are part of the same interconnected network of CI does not invest in adequate security measures, the downstream effects of a cascading

failure would make one's own investments in security futile. A "tipping point" can be reached in both a positive and negative manner; if enough key player elect to invest in their CI resiliency, more will follow, and the reverse holds true as well (Heal et al. 2006).

When self-regulation cannot produce a sufficiently resilient CI environment, third-party intervention may be the last resort. Governments hold significant sanctioning power in the form of legislation, which can be directed via fines, revoked business licenses, and even criminal prosecution. An international survey of IT executives sheds light on the belief that a strong majority of them believe government regulation provides a significant improvement to cyber security (Baker et al. 2010). While the driving force of government regulation may be conducive to an improved atmosphere of CI security, "Overregulation or prescriptive regulations will damage growth. Deregulation and market forces usually produce better economic outcomes, but there are issues—consumer safety or national defense—where the market response will always be inadequate" (Lewis 2011: 5). That is to say that too much government regulation can hinder the private sector's ability to sustain the business growth it needs to remain ahead of the curve when it comes security issues, but that this need for growth cannot supersede the social values which reflect a strong and safe society. As such, a delicate balance between regulation and business growth (which entails a certain degree of risk), must be struck in order to have any chance of making CI as resilient as it can be. When international and state/provincial borders, and their respective legal frameworks get involved, the issue of government regulation becomes all the more convoluted. Policy and law conflict with one another, and the regulatory force held by independent government bodies weakens as a result. Without coordination effort, and consistency of enforcement, inter-jurisdictional regulatory frameworks are apt to fail just as much as interdependent private sector CI operators are to suffer the consequences of cascading failures due to their complacency with regards to security investments.

Summary

Critical infrastructure in Canada is faced with many types of threats, caused by nature or by mankind. Cyber security has been pulled to the forefront of the collective mindset of CI operators and government bodies alike due to the degree of damage that can be done to multiple systems at once. The so-called interdependencies across CI sectors may not be subject to the dramatized fear of a complete domino-style collapse, but there is still a risk present to multiple CI operators at once when one or more related firms choose not to secure their infrastructure adequately. Thus, it is important to find ways to incentivize these CI operators to invest proactively in the security and resilience of their assets for the benefit of society as a whole. Difficulties arise when it comes to sharing information between private sector firms as a result of a cut-throat competitive culture that deters openness and transparency. Even in the public sector, where these values are supposed to be espoused, jurisdictional disputes over policy and law can hinder progress in coordinating and regulating the practices necessary to ensuring that CI is adequately prepared to deal with hazards of all kinds. The sum of it all is that, if left to its own devices, the conditions necessary for a safe and secure critical infrastructure network in North America are untenable. In such a complex environment, where infrastructures are dependent upon one another to function and society has a stake in their continuous operation, there is a shared responsibility between private and public actors to work collaboratively towards that goal.

The final section of this paper introduces the *Beyond the Border Action Plan* (BtB for short), an initiative conceived in 2011 to tackle the very issues that have just been discussed. An explanation of the BtB and its affiliated sub-initiatives will be provided, in addition to an analysis of its application in relation to the theories on trust and coordination of governance networks discussed in the first section of this paper. This section has served to provide the contextual information to help situate the current issues and dilemmas faced by critical infrastructure and will be very useful for the case study that follows.

Part Three: *Beyond the Border* – An International Exercise in Meta-Governance

Introduction to Part Three: What is the Beyond the Border Action Plan?

Threats to critical infrastructure transcend national borders and any other social construct developed by humans. The types of hazards present in southwestern New Brunswick would be no different than those in northern Maine. It makes little sense to avoid cooperating with one's neighbour when combined resources can address and respond to threats to CI more effectively. This is the mentality behind the *Beyond the Border Action Plan* (henceforth referred to as "BtB"). On February 4, 2011, Prime Minister Stephen Harper and President Barack Obama agreed upon a joint framework for dealing with the common issues that transcend our national borders. The BtB action plan consists of 34 initiatives under three distinct categories: border security, facilitation of trade and economic growth, as well as critical infrastructure protection and cyber security (Canada 2011). It is as much a plan for national security as it is for economic prosperity for both Canada and the United States. For the purposes of this paper, however, only the issues of critical infrastructure and cyber security will be addressed, as the subjects of border security and trade fall outside the scope of its area of study.

The BtB has six clearly-defined initiatives under its critical infrastructure protection segment, which consist of:

1. Enhancing Cross-Border Critical Infrastructure and Resilience
2. Government and Digital Infrastructure - Strengthening Cyber Security
3. Expanding Joint Leadership on International Cyber Security Efforts
4. Mitigating the Impacts of Disruptions on Communities and the Economy
5. Enhancing Preparedness for Health Security Threats
6. Emergency Management CBRNE and Interoperability

In addition, the BtB includes two distinct initiatives that relate to its governance framework:

1. BtB Governance and Oversight - Executive Steering Committee
2. Developing a Statement of Privacy Principles and Practices (Public Safety Canada 2014)

There is an intricate coordination model designed for the BtB. For both Canada and the United States, each of these initiatives is tied to a relevant department or agency which acts to support and coordinate the applicable stakeholders across the public and private sectors. However, the higher-level, more overarching role of coordinating all of these initiatives falls under the purview of Public Safety Canada, and the Department of Homeland Security in the United States, with an Executive Steering Committee comprised of high-ranking public officials acting as the bridge between them. In a sense, the Executive Steering Committee plays the role of meta-governor for the broader BtB initiative, but each of the initiatives listed above has a slew of underlying action plans and strategies designed to tackle the lower-level issues that must be addressed in order for it to succeed as a whole. For instance, there is the *National Strategy for Critical Infrastructure* and its accompanying *Action Plan for Critical Infrastructure*, the *Action Plan 2010-2015 for Canada's Cyber Security Strategy*, the *Cybersecurity Action Plan Between Public Safety Canada and the Department of Homeland Security*, in addition to the *Canada-U.S. Resiliency Experiment* series (CAUSE). In that sense, each of the smaller sub-initiatives that make up the larger BtB action plan can be considered as individual governance networks, populated by public and private sector stakeholders, sorted by their relevant knowledge, expertise, and resources which are pertinent to their own subset of issues.

Viewing the BtB through this lens allows for a case study which links to the theoretical concepts discussed in the first section of this paper, and to test the hypothesis that effective meta-governance requires building trust amongst partners in a network, and that this is achieved through a balance of process design and institutional management. Furthermore, the notion of investing in critical

infrastructure protection can be linked to the topic of corporate social responsibility as it was discussed earlier in the paper. As such, the following section will explore the BtB initiative as an exercise in international meta-governance and to demonstrate how such a collaborative endeavour requires trust to be forged through strategic management of the many different governance networks that are involved in its mission. The first part will shed light on the value placed on information sharing throughout the myriad of governance networks that make up the BtB's critical infrastructure component, and which meta-governance tools and strategies have been made available to enable said sharing of information. The next section will elaborate on how the BtB depends heavily on fostering trust in its member stakeholders as a means of sustaining the surprisingly fragile framework of governance developed between Canada and the United States. Finally, the discussion will end on the topic of corporate social responsibility and its relevance to trust between CI actors in multiple governance networks. This is by no means a critical assessment of the performance of the BtB initiative and should not be misconstrued as such; the aim here is to use the BtB as source of evidence to highlight the real-world applications of the theoretical concepts surrounding meta-governance as they have been presented.

Sharing Information with *Beyond the Border*

At its very core, the BtB initiative demands a certain level of information exchange which goes beyond what would ordinarily be expected of individual CI operators and government bodies. Information, which includes anything from threat assessments to data on the operational capacities of various systems used by CI operators, is the "fuel" which sustains the activities of the complex governance networks which make up the BtB. Earlier in this paper, the primacy of information as a resource in governance networks was discussed. Crozier and Friedberg (1980) address the topic of information in terms of strategic bargaining between actors where positioning oneself with privileged information puts one at a notable advantage over others. When dealing with an issue as urgent and

sensitive to the public wellbeing as CI protection and resiliency, this mentality of strategic positioning and conflict over information needs to be washed out. As Rudner (2008: 16) points out, the CI community "should undergo an organizational-cultural shift from the traditional reticence based on 'need to know' to a recognition of the 'need to share' pertinent information". However, there are two elements of information sharing that need to be delicately balanced in order for it to be fruitful to the cause of securing CI: continuous, unhindered and rapid flow of information between relevant actors, and the protection of sensitive information from unscrupulous entities.

Let us first start by addressing the former issue, ensuring the consistent and expeditious transfer of information between actors. The 2014-2017 *Action Plan for Critical Infrastructure* distinguishes between two types of scenarios where information sharing is to be considered under a different set of priorities: emergency situations and regular situations. Under emergency situations, speed of transfer and accuracy of information is prioritized above all else. Addressing this problem under the BtB is CAUSE, which are a series of cross-border simulations designed to test the capabilities of CI operators and public officials to respond to situations of crisis using the combined resources of both Canada and the United States. One instance of these, the CAUSE II experiment, simulated an oil refinery fire in Saint John, NB and a natural gas explosion near the Maine-New Brunswick border. The purpose of the exercise was to test the interoperability of the main first-responder situational awareness systems used by each province/state in order to determine the effectiveness of information exchange in real-time (Department of Homeland Security 2015; Vallerand et al. 2013). The simulation of a natural disaster impacting the energy sector and the safety of the public revealed the primacy of information sharing as a guiding principle to these exercises. In fact, a number of the findings and recommendations outlined in the CAUSE II final report refer to information exchange and partnership building as essential criteria for an effectively coordinated cross-border emergency response. On the topic of information sharing and partnerships, this is what the report had to say: "The willingness to trust and rely on the information

that is shared and exchanged during an event will be determined by the strength of the partnerships that exist prior to the occurrence of emergency events" (Vallerand et al. 2013: 28).

The CAUSE II experiment has one drawback in that it was primarily focused on the involvement of partnering public sector entities, with little to no involvement from the private sector. While this limits its usefulness in discussing information sharing in governance networks featuring public-private partnerships, there is still something to be learned from it. The CAUSE II report suggests that some of the data gathering tools belonging to the public sector can be used by the private sector for the purposes of adapting to prevent or mitigate the impacts of future disasters and to develop improved business continuity processes (Vallerand et al. 2013). This aligns with Shore's (2008: 7) argument that "Private sector CEI [Critical Energy Infrastructure]-related companies must have enough information to make sensible risk assessments on which to base their planning and allocate their resources". There is a certain expectation that the public sector, with its significant resources for gathering information which could be relevant to a private sector CI company's ability to protect its infrastructure, must share its acquired knowledge openly with its partners in both the public and private sectors. This goes back to Branscomb and Michel-Kerjan's (2006) distinction of *operational information* and *intelligence*; here, government bodies serve to provide intelligence to the CI community so that it may react accordingly. Doing so benefits society as a whole and serves as an important step in building strong partnerships, and therefore, more effective governance networks.

On the other hand, it would be foolish to claim that information should only be provided by the public sector in a governance network focused on CI protection. Where the expectation of greater private sector involvement in information sharing arises is under so-called "regular situations" - that is to say, in the day-to-day dealings of public and private actors in their respective CI networks. It is understandable that during emergencies businesses will be less apt to divulge potentially sensitive information due to uncertainty surrounding the privacy standards in such circumstances. Under no such

pressures, there is no reason why cross-sector partnerships such as the BtB cannot involve private sector entities sharing information with each other and with their public sector affiliates. The information offered by the private sector is deemed *operational information* and can likewise be used by partners to perform appropriate risk assessments and identify vulnerabilities within a sector. The spread of information builds a greater sense of awareness of the present landscape of CI, which "increases the overall perception of the risks related to critical infrastructure protection, helping critical infrastructure operators and other stakeholders to prioritize the risks while enacting smoother and cost-effective policies and crisis management procedures" (Ward et al. 2014: 194).

Part of the meta-governor's role in managing governance networks is to facilitate productive communication between actors. Because government bodies like Public Safety Canada and the Department of Homeland Security are regarded as meta-governors in the BtB initiative, they therefore have a responsibility to provide the necessary framework for active discussion and exchange of information between public and private sector groups. In essence, due to the scale of the BtB and all of its sub-initiatives, the role of the government as meta-governor cannot be strictly confined to direct supervision and control, but instead must be directed at "coordinating networks and selecting instruments that can be used to motivate these networks for CIP [critical infrastructure protection] tasks" (Dunn-Cavelty and Suter 2009: 180). The BtB exemplifies this approach through the implementation of two distinct mechanisms for communication. First, under the *National Strategy for Critical Infrastructure* (2014), there is the establishment of the National Cross-Sector Forum, which serves to rally all of the individual CI sector networks (each with their own forum) and to spark discussion on issues pertinent across multiple sectors as well as identifying cross-sector interdependencies. Participation in these networks is voluntary and designed to bring CI operators and relevant public sector groups together for face-to-face interaction. With that said, the National Cross-Sector Forum can be used simultaneously as a meta-governance tool for process design as much as it

can for institutional management. That is to say, government bodies acting as meta-governors for their respective sectors can use the forums to promote the sharing of ideas and build a healthy amount of conflict and consensus which is necessary for any governance network (i.e. process design). At the same time, these meta-governors can choose to control membership of these forums if they feel that innovation and engagement is being stifled by uncooperative members - an institutional management approach to meta-governance.

Another tool created to assist in achieving the BtB's information-sharing goals is the Canadian Critical Infrastructure Information Gateway ("CI Gateway"). The CI Gateway is a tool developed through the *Action Plan for Critical Infrastructure* and it is a web-based portal used as a repository for reports and analytics from public and private sector entities which are made open to be shared for ease of access and relative transparency. While the goal behind the CI Gateway is worthy of praise, it still faces the issue that CI organizations are normally very reluctant to share information about their systems due to their nature as a target for malicious attacks (Chang et al. 2014). Adding to this is the fact that businesses tend to downplay the effects of cascading failures affecting other businesses down the line (Van Eeten 2011; Kunreuther and Heal 2003; Heal et al. 2006), making the CI Gateway a successful operation a difficult challenge. The result is a "market failure" with regards to information which prevents individual infrastructure operators from understanding how resilient their systems are in the web of interdependent infrastructures (Chang et al. 2014). Once again, this is where meta-governance can fill in the gap where the private sector has lacked the incentive to produce and share information for the benefit of the CI community. Berke and Campanella (2006) speak to the effectiveness of having government organizations acting as intermediaries to assist with fostering cooperation and collaboration with actors who may have never previously worked together. Linking this to meta-governance, a department such as Public Safety Canada can apply a process design strategy by leveraging its resources and those of other government departments to generate intelligence (e.g.

severe weather warnings, potential terrorist threats, etc.), which can then be used by private CI operators to react appropriately. This goes back to Mauss's (2007) notion of "the gift", as it was presented earlier in this paper; CI operators receive the "gift" of intelligence information from the public sector and arguably have an obligation driven by social pressures (Dandurand 2012) to repay said gift by sharing their own proprietary information and expertise on sector-specific issues. Thus, by seeding the CI Gateway with intelligence information, Public Safety Canada and other related agencies can arguably foster a greater sense of collaboration between public and private sector actors.

Building Trust Through Meta-Governance in the CI Sector

The discussion on sparking collaboration between the public and private sector to share information via the National Cross-Sector Forum and the CI Gateway has thus far neglected to touch on one critical topic: trust. It is one thing to build a trusting relationship between a private sector CI operator and the government, but to replicate that with multiple partners across a number of different sectors and even international borders is another matter altogether. As discussed in the previous section, private sector CI operators are especially reluctant to share information with each other as a result of business competition and security. The forums and the CI Gateway, therefore, are prone to devolve into stagnancy and ineffectiveness - a condition in which no governance network should ever want to find itself. High levels of uncertainty caused by a lack of information about the environment in which CI operators engage leads to elevated transaction costs, which is at the root of governance networks falling apart.

Before the BtB was conceptualized, Martin Rudner (2008: 7) pointed out that the Government of Canada had not yet established a "centralized, national clearinghouse for information". With the CI Gateway, this concern has been addressed but the exercise in populating this clearinghouse of information hinges entirely on CI operators and public sector groups trusting each other enough to

share their information in the first place. The issue lies in actors justifiably mistrusting the technology behind something like the CI Gateway and its potential for misuse. In their study of the *European Reference Network for Critical Infrastructure Protection*, David Ward et al. (2014) found that trust played a crucial role in promoting the participation of CI actors in a technological environment, but that this trust was developed in stages. The three-stage approach they defined consists of first building trusting relationships at the personal level (i.e. face-to-face meetings), which for the BtB is achieved through the National Cross-Sector Forum. After this is achieved, the second step would involve building trust in the institutions and organizations themselves. Building organizational relationships based solely on financial incentives is not enough to create what Koski (2011) refers to as the "policy glue" needed to hold a complex network of actors together. The final step, which complements the previous one, is the use of technology to facilitate communication and the spread of information between actors. In essence, trust in technology cannot be maintained adequately until personal trust and trust in institutions is achieved. The author sums up this idea nicely: "In practice, personal trust can lead to trust in institutions that, in turn, can deliver trust in technology, which may then increase personal trust through increased information disclosure" (Ward et al. 2014: 197). Trust is therefore a cyclical attribute to a healthy governance network. Due to the sensitive and exclusive nature of an instrument like the CI Gateway, it is not possible to assess how healthy the information sharing network truly is, but based on the criteria above, the BtB has all the meta-governance tools present to build that trust through at least the first and final stages of the trust building process. However, for the second stage - building trust in institutions and organizations - success is determined by achieving the appropriate balance of "hard" and "soft" meta-governance strategies (i.e. institutional management and process design) and creating the correct governance framework to sustain that trust. What follows is a discussion on the significance of transaction costs as they relate to trust in institutions and organizations within the BtB initiative, and how proper meta-governance can keep said transaction costs down.

Transaction Costs and Trust with *Beyond the Border*

One of the notions which was elaborated in the first section of this paper was the conditions which can lead to failure of governance networks. In that section, it was stated that elevated transaction costs produce situations where cooperation between members of a group is reduced due to a greater degree of risk and uncertainty with regards to how another partner will behave when presented with a situation of expected reciprocal exchange (i.e. will they behave in a manner that is trustworthy, or opportunistically?). The BtB is a prime example of a governance network faced with such dilemmas on a regular basis, as the information being exchanged by members in a group can be incredibly valuable, and so are the many opportunities to shirk responsibility for investing in security measures of CI. The goal of the meta-governor in this instance is to provide the right amount of regulatory heft to prevent opportunistic behaviour in the network whilst simultaneously keeping interactions free enough that it is not cumbersome to engage in open exchanges.

An argument presented by Shore (2008) is that government and the private sector have a "legal imperative" to protect CI against threats, which would imply legal liability in the event of damage resulting from a catastrophe that could have been avoided. This is what Kirton and Guebert (2010) refer to as “hard law”, which is a form of legally entrenched regulatory power where non-compliance to predefined rules results in judicial sanctions, enforceable by laws, treaties and other enforceable agreements. In theory, this threat of legal sanction should provide ample incentive for government and private sector actors alike to invest adequately in security measures and to perform their due diligence with regards to sharing information which could be essential for another actor to protect their own assets. Because the BtB is an international initiative which must take into account the policies and laws from a multitude of jurisdictions including federal and state/province legislation, relying strictly on such a "legal imperative" to motivate actors to engage actively and responsibly is unsustainable. This argument is further supported by Kirton and Guebert (2010), who suggest that “soft law” (i.e.

regulations which are not legally binding but still enforceable from a social/political sense) has been more successful in North America at filling in the gaps where hard law is incapable or ineffective at maintaining compliance and policy collaboration, citing NAFTA as an example. Instances of applied soft law can be found through workshops, forums, and task forces, as well as even softer mediums such as e-mails and informal meetings (Gattinger and Hale 2010).

With regards to the BtB, there is evidence that a soft law approach has been developed to serve as a more flexible alternative to the existing laws and treaties which reside in their respective national and provincial/state jurisdictions. Canada and the United States have created what is called the Regulatory Cooperation Council (RCC), which is designed to "to facilitate closer regulatory cooperation between our two countries and enhance economic competitiveness by aligning our regulatory systems where appropriate while maintaining high levels of protection for health, safety and the environment" (Canada 2015). Under this, twelve separate Regulatory Partnership Statements (RPS) have been created to enhance coherence when it comes to regulatory bodies in fields ranging from health, to the environment, and to transportation (Embassy of the United States 2015). In essence, these partnerships aim to harmonize policies related to the safety of both Canada and the United States by gathering all related public and private sector entities to ensure uniform compliance. While the RCC is still considered a form of soft law (it is not an official treaty), it does not offer the same flexibility nor the same ease of interaction between actors as, say, the National Cross-Sector Forum or the CI Gateway, which are much softer on the spectrum of hard and soft law. Such a regulatory framework as the RCC may indeed be helpful towards enforcing compliance with the many laws and policies that govern CI, but as was argued earlier in the paper, too much reliance on regulation in a governance network can gradually lead to elevated transaction costs between actors who now must tip-toe carefully around a cluster of rules and laws in order to avoid facing potential sanctions for their actions. This is one of the consequences of too great a focus on an institutional management approach to meta-governance.

Furthermore, such a cross-border regulatory body is at risk of creating situations where one regulatory entity which has adopted a more "hands-on" approach to managing governance networks in a particular sector inadvertently imposes its rules above those of its counterpart regulatory entity, leading to potential conflicts and sub-optimal policy coherence between both countries. In her research following policy collaboration in the energy sector, Gattinger (2011) provides an empirical example of this exact scenario using the Federal Energy Regulatory Commission (FERC) and the North American Energy Reliability Corporation (NERC). In her example, FERC is the one adopting the institutional management approach – it is actively involved in monitoring and ensuring compliance with NERC standard - whereas the Canadian regulatory counterparts have a more "hands-off" process design approach, which results in FERC having a greater influence over the policy landscape managed by NERC. Thus, even in the area of policy collaboration, the RCC under the BtB must be wary of such unwanted imbalances of power resulting from disparate styles of meta-governance.

On the subject of power imbalances, a cross-border regulatory framework like the RCC is also subject to further complications from conflicts arising between federal and provincial/state governments as their roles and jurisdictions often overlap in such a nebulous area as critical infrastructure protection. This is especially so in Canada, where federal spending power and conditional transfer payments can potentially centralize the decision-making power with the federal government (Champagne et al. 2014a), thus influencing the playing field while leaving no room for provincial authority to play a part in policy collaboration. For an initiative like the BtB to be successful, it is imperative that the power to create and implement policy not be centralized because this strays away from meta-governance and shifts towards traditional top-down governance which is incompatible with the way the initiative is structured. In other words, the BtB - and critical infrastructure protection more broadly - is a multi-level governance issue and requires the combined resources and full collaboration of

federal, provincial, municipal and non-government actors to achieve successful results (Champagne et al. 2014b).

Even in an arrangement as complex as the BtB, some degree of freedom must be given to actors to do business with one another so as not to impede growth (Lewis 2011). This means adopting a softer process design approach and accounting for some level of risk that actors will not behave in a trustworthy manner. In a study on the relationship between risk and trust, it was discovered that networks where a lot of reciprocal and non-reciprocal exchange take place require a certain degree of risk to be present in order for trust to build between actors (Molm et al. 2009). In other words, if there is no risk for a partner to share valuable information or to invest resources in securing their assets without knowing that the other partner will reciprocate (e.g. in a highly regulated environment where such actions would be heavily sanctioned), then there is no reason for the actors to build a sense of trust for future interactions. In reality, if an actor were to behave opportunistically and misuse shared information or dangerously expose their partner(s) to "contamination" with regards to the interdependency of their infrastructures by not mutually investing in security, the relationship of trust will have been breached and any future exchanges with said actor will be strained, resulting in greater transaction costs. The instruments of engagement like the CI Gateway and the National Cross-Sector Forum depend on high levels of trust between actors, and therefore it falls upon the government as meta-governor to balance its regulatory power of sanction and permitting open relationships founded on trust to flourish between CI operators.

Corporate Social Responsibility and Trust-Building in *Beyond the Border*

Lastly, there is a link to be drawn between corporate social responsibility, trust, and transaction costs as they relate to the BtB initiative. A partnership between Defense Research and Development Canada and Public Safety Canada led to the creation of the Canadian Safety and Security Program (CSSP), which

targets millions of dollars of funding annually towards the development of innovative science and technology projects designed to enhance the resiliency of CI in Canada under the greater BtB action plan (CSSP 2015). For instance, the CSSP recently completed the construction of a National Energy Infrastructure Test Center, which serves as a sandbox environment for testing physical and cyber-security vulnerabilities present in common SCADA systems used by energy infrastructure operators in Canada and around the globe (Howes et al. 2014). If we are to tie this to the notion of corporate social responsibility, one can perceive such an investment as a "gift" which is expected to be repaid by the private sector CI operators in the form of socially responsible business practices. This means using the valuable knowledge gained from the test center's experiments in order to invest adequately in their own physical and cyber resiliency for the benefit of the community of CI operators who happen to be dependent on the smooth operation of their infrastructure, and for society as a whole who also depend on the infrastructure for safety. The targeted nature of these investments by the CSSP seems to fall in line with Van Eeten et al (2011) and their argument that cascading failures tend to stem primarily from the energy and telecommunications sectors, as most of the projects and activities funded by the program are related to these. Thus, the meta-governance strategy adopted by the CSSP by investing in CI security innovation is an example of a process design approach where the fruits of those investments are designed to incentivize the private sector CI community to also invest responsibly in the security of their own assets. If this strategy proves to be successful and a sizeable amount of CI operators are observed to be fulfilling their CSR obligations, the "tipping point" proposed by Heal et al (2006) can be reached and even more will follow from their example. This demonstrates once again that the BtB is an exercise in meta-governance with a built-in component of CSR used to incentivize the CI community to invest in a manner that ensures the safety and security of the community as a whole.

It must not be forgotten that the entire premise of this vision is founded upon the assumption that trust is high across the governance networks involved and that any breach of that trust can

seriously put at risk the entire meta-governance strategy applied here. In other words, if the CSSP continues to invest its resources in programs for the benefit of the CI community, but a few of the members of that community choose to behave opportunistically and disregard their CSR obligations, then the foundation of trust within these governance networks will quickly begin to erode. Transaction costs will then begin to rise in consequence, thus increasing the difficulty for collaborative engagements to take place between members in the CI network. The same can be said about the CI Gateway and the National Cross-Sector forum with regards to information sharing; if certain actors choose to act opportunistically and use the information for personal gain at the expense of the provider, trust as a valuable and finite commodity in a governance network vanishes and transaction costs rise for all future interactions. In these situations, the meta-governor would have to step in and apply an institutional management approach to re-stabilize the network environment, which implies the use of regulation and coercion - two activities which have already been labelled as constricting to the growth of business and to the overall health of a governance network. Strategies such as these could involve barring access to certain actors from the CI Gateway or National Cross-Sector Forum, or to avoid investment of public funds for programs directed at companies who have proven to be untrustworthy. It comes down to creating an environment where building trust-based relationships is facilitated and where abuses of said relationships is met with consequences to prevent transaction costs from sullying the spirit of cooperation and collaboration which is essential to healthy governance networks.

Summary

To put things to a close, the BtB is an excellent example of the theory and practice of meta-governance at play in the field of critical infrastructure. Through a number of the various programs and activities which fall under the greater "umbrella" of the BtB, including the CAUSE resiliency experiments, the National Cross-Sector Forum, the CI Gateway, as well as the Canadian Safety and Security Program, it was shown how the initiative makes use of the full spectrum of meta-governance strategies (process

design and institutional management). Meta-governance and the balance of its different approaches are revealed to be necessary in building governance networks where trust is plentiful and low transaction costs encourage appropriate CSR behaviour amongst partners in both the public and private sectors. Furthermore, the dangers of violations of that trust were explored through potential scenarios faced by the initiatives under the BtB. Overall, as the BtB moves forward, it will continue to serve as an excellent case study in the real-world application of meta-governance, proving the intrinsic value of trust in governance networks as a measure of success in policy implementation.

Conclusion

Building trust through meta-governance is a challenging process. There is a delicate balance to be achieved between implementing process design and institutional management approaches in order to ensure that actors are able to still interact with a great degree of freedom, while still being able to regulate against corrosive behaviours that hinder the development of trust. The paper began by providing the theoretical considerations of meta-governance, trust, transaction costs and corporate social responsibility and how these are all interrelated. Following that, some contextual information was given about the threats and vulnerabilities present in the field of critical infrastructure. There was discussion about the level of interdependencies which exist between the various CI sectors and the primacy of cyber security in the modern context of protecting CI. Finally, the theory of meta-governance and the contextual information on CI vulnerability culminated into a discussion on the *Beyond the Border* action plan.

The *Beyond the Border* initiative was used to show some elements of the practice of meta-governance, including the importance of information sharing, building trust and how to incentivize the private sector to invest proactively in security. It was also explored how corporate social responsibility serves as the keystone for sustaining trust in a CI governance network; socially responsible behaviour on behalf of private sector CI operators contributes to a greater overall sense of trust in the network, which keeps transaction costs low and perpetuates the lack of necessity for direct government intervention. Many of the elements of *Beyond the Border*, such as the CI Gateway, the CAUSE resiliency experiments, the National Cross-Sector Forum and the Canadian Safety and Security Program's targeted investments are all examples of meta-governance at work and truly showcases the critical nature of trust to sustain these programs. In the absence of a strong foundation of trust between CI actors, the system breaks down and is forced to return to a state of strict regulation to ensure the safety and protection of society.

At the time of writing this, *Beyond the Border* is still fairly early into its development and many of its goals and objectives are still in-progress. Further still, some new sub-initiatives are bound to spring up as a result of the very dynamic and constantly shifting nature of critical infrastructure protection. Thus, there is still a wide body of research potential to be tapped from this initiative from a public administration perspective. Future considerations for research could involve studies of the governance model, most notably with the Executive Steering Committee and the Regulatory Cooperation Council and how policies and laws are aligned between Canada and the United States for CI protection. Another potential avenue for research would be a performance assessment of the success for the various initiatives under the greater *Beyond the Border* strategy. There is plenty of potential for academic efforts to be applied on CI initiatives like this one and the value these studies present for the field of public administration is quite high indeed.

Bibliography

Auerswald, P., La Porte, T., La Porte, T., & Michel-Kerjan, E. (2006). Where Private Efficiency Meets Public Vulnerability: The Critical Infrastructure Challenge. In P. Auerswald, T. La Porte, T. La Porte, & E. Michel-Kerjan, *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability* (pp. 3-16). Cambridge: Cambridge University Press.

Baker, S., Waterman, S., & Ivanov, G. (2010). *In the Crossfire: Critical Infrastructure in the Age of Cyber War.* London: McAfee International Ltd.

Benoit, J. (2014). *Assessing Security Threats to Canada's Energy Infrastructure: The Enbridge Northern Gateway Pipeline.* Burnaby, BC: Simon Fraser University.

Berke, P., & Campanella, T. (2006). Planning for Postdisaster Resiliency. *The Annals of the American Academy*, 192-207.

Bernier, L., & Simard, L. (2005). The Governance of Public Enterprises: Challenges in a Brave New World. *Cahier de recherche du Centre de recherche sur la gouvernance des entreprises publiques et l'intérêt général (CERGO)*, 1-18.

Brans, M. (1997). Challenges to the practice and theory of public administration. *Journal of Theoretical Politics, Vol. 9(3)*, 389-415.

Branscomb, L., & Michel-Kerjan, E. (2006). Public-Private Collaboration on a National and International Scale. In P. Auerswald, T. La Porte, T. La Porte, & E. Michel-Kerjan, *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability* (pp. 395-403). Cambridge: Cambridge University Press.

Canada. (2011). *Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness.* Ottawa: Government of Canada.

Canada. (2015, September 20). *Regulatory Cooperation Council*. Retrieved from Canada's Economic Action Plan: http://actionplan.gc.ca/en/content/regulatory-cooperation-council

Canadian Safety and Security Program (CSSP). (2015, September 14). *Funding Categories*. Retrieved from Science.gc.ca: http://www.science.gc.ca/default.asp?lang=En&n=D9163BB5-1

Canadian Security Intelligence Service (CSIS). (2015, September 3). *1995 Public Report and Program Outlook.* Retrieved from http://www.datapacrat.com/True/INTEL/CSIS/PUB1995E.HTM

Castells, M. (1996). *The rise of the network society.* Cambridge: Blackwell Publishers.

Champagne, E., Choinière, O., & Maxwell, E. (2014). Le financement des politiques publiques au Canada. In M. Leroy, & G. Orsoni, *Le financement des politiques publiques* (pp. 429-457). Bruxelle: Editions Bruylan/De Boeck.

Champagne, E., Maxwell, E., Koskela, E., & Rheault, G. (2014). *Collaborative Resilience in Critical Infrastructure and Crime Prevention: A Discussion Paper.* Ottawa: Center on Governance Research Paper Series.

Chang, S., McDaniels, T., Fox, J., Dhariwal, R., & Longstaff, H. (2014). Toward Disaster-Resilient Cities: Characterizing Resilience of Infrastructure Systems with Expert Judgments. *Risk Analysis 34(3)*, 416-434.

Clarke, R. A., & Knake, R. K. (2012). *Cyber War: The Next Threat to National Security and What to Do About It.* New York: HarperCollins.

Considine, M., & Lewis, J. (2003). Bureaucracy, Network or Enterprise? Comparing Models of Governance in Australia, Britain, the Netherlands, and New Zealand. *Public Administration Review*, 131-140.

Crozier, M., & Friedberg, E. (1980). *Actors and Systems: The Politics of Collective Action.* Chicago: University of Chicago Press.

Dandurand, G. (2012). La responsabilité sociale des entreprises est-elle sociale? *Thèse de maîtrise, École de développement international et mondialisation, Université d'Ottawa*, 1-106.

De Bruijne, M., & van Eeten, M. (2007). Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. *Journal of Contingencies and Crisis Management, Vol. 15 (1)*, 18-29.

De Pierrebourg, F., & Juneau-Katsuya, M. (2010). *Nest of Spies: The Startling Truth about Foreign Agents at Work WIthin Canada's Borders.* New York: HarperCollins.

Department of Homeland Security. (2015, August 24). *Interoperable Communications Across Borders*. Retrieved from Department of Homeland Security: http://www.dhs.gov/interoperable-communications-across-borders

Dunn-Cavelty, M., & Suter, M. (2009). Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, 179-187.

Edelenbos, J., & Klijn, E.-H. (2007). Trust in Complex Decision-Making Networks: A Theoretical and Empirical Exploration. *Administration & Society, Vol. 39(1)*, 25-50.

Embassy of the United States. (2015, September 20). *United States and Canada Announce Regulatory Partnership Statements and Annual Work Plans*. Retrieved from Embassy of the United States in Ottawa: http://canada.usembassy.gov/news-events/2015-news-and-events/may-2015/28-may-2015-united-states-and-canada-announce-regulatory-partnership-statements-and-annual-work-plans.html

Farneti, F., Padovani, E., & Young, D. (2010). Governance of Outsourcing and Contractual Relationships. In S. P. Osborne, *The New Public Governance? Emerging pespectives on the theory and practice of public governance* (pp. 255-269). New York: Routledge.

Gattinger, M. (2011). Canada-United States Electricity relations: Test-Bed for North American Policy Making? *Canadian-American Public Policy No. 77*, 1-41.

Gattinger, M., & Hale, G. (2010). Chapter 1: Borders and Bridges: Canada's Policy Relations in North America. In M. Gattinger, & G. Hale, *Borders and Bridges: Canada's Policy Relations in North America* (pp. 1-18). Don Mills, Ontario: Oxford University Press.

Gendron, A. (2010). *Critical Energy Infrastructure Protection in Canada.* Ottawa: Canadian Centre of Intelligence and Security Studies.

Graham, A. (2011). *Canada's Critical Infrastructure: When is Safe Enough Safe Enough?* Ottawa: The Macdonald-Laurier Institute.

Haas, P. M. (2004). When does power listen to truth? A constructivist approach to the policy process. *Journal of European Public Policy*, 569-592.

Hall, P. (1993). Policy Paradigms, Social Learning, and the State: The Case of Economic Policymaking in Britain. *Comparative Politics, 25(3)*, 275-296.

Hay, J. B. (2006). *Who Does What? Critical Infrastructure Protection in the Canadian Government.* Ottawa: Canadian Centre of Intelligence and Security Studies.

Heal, G., Kearns, M., Kleindorfer, P., & Kunreuther, H. (2006). Interdependent Security in Interconnected Networks. In P. Auerswald, L. Branscomb, T. La Porte, & E. Michel-Kerjan, *Seeds of Disaster, Roots of Response: How Private Action can Reduce Public Vulnerability* (pp. 258-275). Cambridge: Cambridge University Press.

Howes, R., Hales, D., & Vallerand, D. (2014). *National Energy Infrastructure Test Centre (NEITC): Concept and Development of an Entity to Assist in Cyber Protection of Industrial Control Systems within the Energy and Utilities Sector in Canada.* Ottawa: Defence R&D Canada - Center for Security Studies.

Kickert, W., Klijn, E., & Koppenjan, J. (1997). *Manging Complex Networks.* London: Sage.

Kirton, J., & Guebert, J. (2010). Chapter 4: Soft Law, Regulatory Coordination, and Convergence in North America. In M. Gattinger, & G. Hale, *Borders and Bridges: Canada's Policy Relations in North America* (pp. 59-76). Don Mills, Ontario: Oxford University Press.

Klijn, E., & Koppenjan, J. (2004). *Managing Uncertainties in Networks: A Network Approach to Problem Solving and Decision-making.* London: Routledge.

Klijn, E.-H. (2010). Trust in governance networks: Looking for conditions for innovative solutions and outcomes. In S. P. Osborne, *The New Public Governance? Emerging perspectives on the theory and practice of public governance* (pp. 303-321). New York: Routledge.

Klijn, E.-H., & Edelenbos, J. (2007). Meta-governance as Network Management. In E. Sorensen, & J. Torfing, *Theories of Democratic Network Governance* (pp. 199-214). New York: Palgrave Macmillan.

Koppenjan, J. F. (2007). Consensus and Conflict in Policy Networks: Too Much or Too Little. In E. Sorensen, & J. Torfing, *Theories of Democratic Network Governance* (pp. 133-152). New York: Palgrave Macmillan.

Koski, C. (2011). Committed to Protection? Partnerships in Critical Infrastructure Protection. *Journal of Homeland Security and Emergency Management 8(1)*, 1-18.

Kunreuther, H., & Heal, G. (2003). Interdependent Security. *Journal of Risk and Uncertainty, Vol. 26 (2)*, 231-249.

Lafree, G., Dugan, L., & Miller, E. (2015). *Putting Terrorism in Context: Lessons from the Global Terrorism Database.* London: Routledge.

Lagadec, E. (2009). *Leadership in Unconventional Crises, a Transatlantic and Cross-Sector Assessment.* Washington, DC: Center for Transatlantic Relations.

Lagadec, P., Michel-Kerjan, E., & Ellise, R. (2006). Disaster via Airmail: The Launching of a Global Reaction Capacity After the 2001 Anthreax Attacks. *Innovations*, 99-117.

Lewis, J. A. (2011). *Cybersecurity Two Years Later: A Report of the CSIS Comission on Cybersecurity for the 44th Presidency.* Washington, DC: Center for Strategic and International Studies.

Likar, L. (2011). *Eco-Warriors, Nihilistic Terrorists & the Environment.* Denver, Colorado: Praeger.

Lindblom, C. (1959). The science of "muddling through". *Public Administration Review*, 79-88.

Mauss, M. (2007). *Essai sur le don: Forme et raison de l'échange dans les sociétés archaïques.* Paris: Presses universitaires de France.

McAfee Foundstone Professional Services and McAfee Labs. (2011). *Gloval Energy Cyberattacks: "Night Dragon".* Santa Clara: McAfee Inc.

Molm, L. D., Shaefer, D. R., & Collett, J. L. (2009). Fragile and Resilient Trust: Risk and Uncertainty in Negotiated and Reciprocal Exchange. *Sociological Theory 27(1)*, 1-32.

National Information Sharing Consortium (NISC). (2015, August 18). *What is the Canada-U.S. Enhanced Resiliency Experiment (CAUSE)?* Retrieved from National Information Sharing Consortium: http://www.nisconsortium.org/partner-highlights/736-2/

Noonan, T., & Archuleta, E. (2008). *The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures.* N/A: Department of Homeland Security.

Nooteboom, B. (2002). *Trust: Forms, Foundations, Functions, Failures and Figures.* Cheltenham: Edward Elgar Publishing.

Office of Critical Infrastructure Protection and Emergency Prepardness (OCIPEP). (2003). *Threats to Canada's Critical Infrastructure.* Ottawa: Office of Critical Infrastructure Protection and Emergency Prepardness.

O'Toole, Jr, L. J. (2007). Governing Outputs and Outcomes of Governance Networks. In E. Sorensen, & J. Torfing, *Theories of Democratic Network Governance* (pp. 215-230). New York: Palgrave Macmillan.

Peters, B. (2010). Meta-governance and public management. In S. P. Osborne, *The New Public Governance? Emerging perspectives on the theory and practice of public governance* (pp. 36-51). New York: Routledge.

Public Safety Canada. (2009). *National Strategy for Critical Infrastructure.* Ottawa: Public Safety Canada.

Public Safety Canada. (2013). *Action Plan 2010-2015 for Canada's Cyber Security Strategy.* Ottawa: Public Safety Canada.

Public Safety Canada. (2014). *Action Plan for Critical Infrastructure (2014-2017).* Ottawa: Public Safety Canada.

Public Safety Canada. (2014). *Report on the Beyond the Border Action Plan: Horizontal Initiative for 2011-12 and 2012-13.* Ottawa: Public Safety Canada.

Public Safety Canada. (2015, August 20). *Emergency Management Planning Guide 2010-2011.* Retrieved from Public Safety Canada: Public Safety Canada

Public Safety Canada and the Department of Homeland Security. (2014). *Cybersecurity Action Plan Between Public Safety Canada and the Department of Homeand Security.* Ottawa: Public Safety Canada.

Rhodes, R. (1997). *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability.* Buckingham: Open University Press.

Robinson, P., Woodard, J., & Varnado, S. (1998). How Vulnerable is Our Interlinked Infrastructure? Critical Infrastructure: Interlinked and Vulnerable. *Issues in Science and Technology, Vol. 15 (1)*, 61-67.

Rudner, M. (2008). *Protecting Canada's Energy Infrastructure Against Terrorism: Mapping A Proactive Strategy.* Ottawa: Canadian Centre of Intelligence and Security Studies.

Schapp, L. (2007). Closure and Governance. In E. Sorensen, & J. Torfing, *Theories of Democratic Network Governance* (pp. 111-132). New York: Palgrave Macmillan.

Schattschneider, E. (1960). *The Semisovereign people: a realist's view of democracy in America.* New York: Holt, Rinehart and Winston.

Selsky, J., & Parker, B. (2005). Cross-Sector Partnerships to Address Social Issues: Challenges to Theory and Practice. *Journal of Management, 31(6)*, 849-873.

Shakarian, P., Shakarian, J., & Ruef, J. (2013). *Introduction to Cyber Warfare.* Waltham, MA: Elsevier Science Ltd.

Shore, J. J. (2008). The Legal Imperative to Protect Critical Energy Infrastructure. *The Canadian Centre of Intelligence and Security Studies*, 1-16.

Sorensen, E., & Torfing, J. (2007). Introduction: Governance Network Research: Towards a Second Generation. In E. Sorensen, & J. Torfing, *Theories of Democratic Network Governance* (pp. 1-21). New York: Palgrave Macmillan.

Sorensen, E., & Torfing, J. (2007). Theoretical Approaches to Governance Network Failure. In E. Sorensen, & J. Torfing, *Theories of Democratic Network Governance* (pp. 95-110). New York: Palgrave Macmillan.

Sorensen, E., & Torfing, J. (2007). Theoretical Approaches to Metagovernance. In E. Sorensen, & J. Torfing, *Theories of Democratic Network Governance* (pp. 169-182). New York: Palgrave Macmillan.

Taleb, N. (2007). *The Black Swan: The Impact of the Highly Improbable.* New York: Random House.

Vallerand, A., Dawe, P., Forbes, K., Hales, D., Couture, C., O'Donnell, D., . . . Johnson, A. (2013). *A Canada-U.S. Resiliency Experiment (CAUSE RESILENCY II) on Enhancing Trans-Border Resilience in Emergency and Crisis Management Through Situational Awareness Interoperability: Addressing the Beyond the Border (BTB) Action Plan.* Ottawa: Defence R&D Canada - Center for Security Studies.

Van Eeeten, M., Nieuwenhuijs, A., Luiijf, E., Klaver, M., & Cruz, E. (2011). The State and the Threat of Cascading Failure Across Critical Infrastructures: The Implications of Empirical Evidence from Media Incident Reports. *Public Administration Vol. 89 (2)*, 381-400.

Ward, D., Kourti, N., Lazari, A., & Cofta, P. (2014). Trust Building and the European Reference Network for Critical Infrastructure Protection Community. *International Journal of Critical Infrastructure Protection*, 193-210.

Williamson, O. (1996). *The mechanisms of governance.* Oxford: Oxford University Press.