THE INTERDEPENDENT NATURE OF NATIONAL CYBER SECURITY: MOTIVATING PRIVATE ACTION FOR A PUBLIC GOOD

by

Forrest B. Hare
A Dissertation
Submitted to the
Graduate Faculty
of
George Mason University
in Partial Fulfillment of
the Requirements for the Degree
of
Doctor of Philosophy
Public Policy

Committee:

____________________ Rainer Sommer, Chair

____________________ Philip Auerswald

Robert Axtell __________ Robert Axtell

____________________ Greg Rattray, External Reader

James P Pfiffner __________ James P. Pfiffner, Program Dir.

EDWARD RHODES __________ Edward Rhodes, Dean

Date: 10/18/10 __________ Fall Semester 2010
George Mason University
Fairfax, VA

The Interdependent Nature of National Cyber Security: Motivating Private Action for a Public Good

A dissertation submitted in partial fulfillment of the requirements for the degree of
Doctor of Philosophy at George Mason University

By

Forrest Hare
Master of Art
University of Illinois, 1993
Bachelor of Science
United States Air Force Academy, 1990

Director: Rainer Sommer, Associate Professor
School of Public Policy

Fall Semester 2010
George Mason University
Fairfax, VA

DEDICATION

This work is dedicated to the four people who made this degree possible. The first is the visionary Dr. Lani Kass who encouraged and supported my return to school to earn my doctorate. The second two are my parents, Forrest and Helga Hare. All that is good about me is their fault. Most importantly, I dedicate this to my loving wife, Misuk. She is beautiful in every way.

ACKNOWLEDGEMENTS

I would like to thank my family, friends, and colleagues who have made this journey possible. Without their continual encouragement and support over the last five years, I would not have had the power to finish. First and foremost, I must thank my loving wife. Misuk has had to be a single parent for many, many nights and weekends. My children have also been patient with their father and didn't jump into my lap too often (but often enough) while I was studying.

I thank the leadership of the United States Air Force and Dr. Lani Kass who had the vision to bring the Service into the fight of the future and recognized the need to grow leaders knowledgeable in the field of cyber security by funding most of my studies. My current director, Ms. Wenchel, enthusiastically supported my work for the last two years.

The faculty at SPP has provided the analytical tools to enable my research abilities and has pushed me to question conventional wisdom. Beth Eck kept me on the right path for the last four years and graciously helped solve every problem I had. Professors Rudder and Pfiffner forced me to raise my academic standards. My colleagues at SPP, especially Ryan Zelnio, Kay Sullivan, Scott Buchanan, and Jill Rough, have provided guidance and focus. Without the coding expertise of Goldstein from the CSS Department, I could not have created the agent-based model that was instrumental in conducting this analysis.

Finally, I thank my chair Dr. Rainer Sommer, and the other members of my committee, Dr. Auerswald, Dr. Axtell, and Dr. Rattray who all came together to ensure that I could complete the dissertation before having to deploy to support Operation Enduring Freedom. My committee took on a "project" in an area in which none individually was an expert. However, their combined knowledge helped produce what is hopefully an addition to our knowledge on the subject of cyber security.

TABLE OF CONTENTS

Page

Page

Page

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVATIONS

CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CIRC	Cyber Incident Response Center
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
ES-ISAC	Electric Sector Information Sharing and Analysis Center
FBI	Federal Bureau of Investigations
HSPD	Homeland Security Presidential Directive
ICS-CERT	Industrial Control Systems Computer Emergency Response Team
ICSJWG	Industrial Control Systems Joint Working Group
IDSI	Independent Security Investment
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standards or Independent System Operators
NATO	North Atlantic Treaty Organization
NERC	North American Energy Reliability Corporation
NIPP	National Infrastructure Protection Plan
PLS	Private Legal System
PMA	Power Management Administration
US-CERT	United States Computer Emergency Response Team

ABSTRACT

The Interdependent Nature of National Cyber Security: Motivating Private Action for a Public Good

Forrest Hare, Ph.D.

George Mason University, 2010

Dissertation Director: Dr. Rainer Sommer

The federal government relies largely on voluntary actions by the private firms that comprise the nation's critical infrastructure to secure their operations. Several recent reports have highlighted the potential for cyber security externalities if IT and control systems are not more sufficiently secured. This research will employ a mixed methods approach in an effort to extend limited empirical research regarding the problem of national security in cyberspace. The first perspective will employ an agent-based model to analyze the cyber security investment decision in the defense industrial base. The second will be a case study of the information-sharing network between the electricity sector and the federal government.

PART I

The Cyber Component of National Security

1 Introduction

1.1 **<u>The Public Policy Issue</u>.** In April 2009, Pentagon officials disclosed that computer spies had breached the computer systems responsible for diagnosing maintenance problems during flight testing of the military's new joint strike fighter, its costliest weapons program to date (Gorman, Cole, and Dreazen 2009). At approximately the same time, the *Wall Street Journal* also reported that the US electrical grid had been penetrated by spies who had left behind software capable of disrupting power generation and transmission (Gorman 2009). The thread linking these two incidents is that they both occurred through cyberspace. While cyber security has been a growing area of concern for individuals, firms, academic institutions, and at various levels of government, these recent events have highlighted the national security aspects of the cyber vulnerabilities.

Several recent reports have made recommendations for how the nation can become more secure in cyberspace (see, for example, Goodman and Lin 2007; Lewis 2008). The White House cyber policy review even called for the president to appoint a national cyber security policy official and to make cyber security on of his top management priorities (Hathaway 2009). The federal government can advocate and advance many of these recommendations (e.g. better education and R&D). In fact, the Obama administration has the constitutional authority to direct much stronger cyber security actions if the nation is truly at risk from threats in the domain. However, this and all previous administrations have been unprepared to make this policy move. Instead, the administration must rely on voluntary actions by the private firms that comprise the nation's critical infrastructure (CI) to secure their operations until stronger regulation is enacted. Although the voluntary and limited regulatory actions that these firms must take can vary substantially from sector to sector, two important actions should be conducted by all.

According to the National Infrastructure Protection Plan (NIPP), the first action that firms must take is to invest in and implement strong cyber security measures in their IT and control system operations (DHS 2006). From the perspective of the public good of national security, it is not enough for firms to invest to a level of protection that reduces only their financial risks. They must invest to a level that accounts for their inter-connectedness and considers the potential security externalities generated by insufficient investments (DHS 2006). Since these investments are voluntary in most cases, public officials are limited to engaging with firms and encouraging sufficient investment.

The second major activity being promoted by the federal government is private sector participation in an information-sharing and response network (DHS 2006). The composition of actors in this voluntary network is different for each CI sector, but the central information hub in all cases is the Department of Homeland Security (DHS). From the private sector's perspective, this interaction network could provide valuable information on threats, vulnerabilities, and cyber security defenses. From the public sector's perspective, the network would be of value in helping data fusion centers understand current attacks, current vulnerabilities, and defenses that have proven effective. Improved situational awareness also helps decision makers to understand national-level response options and to be able to implement response measures in a timely fashion.

The critical cyber security breaches identified above demonstrate that essential investments needed to secure the nation in cyberspace and help prepare a national crisis response have not occurred. While the legal and policy debates continue on Capitol Hill regarding the costs and benefits of additional regulatory security measures within the nation's critical infrastructure sectors, federal security agencies such as DHS and the FBI must continue to foster private sector contributions to national security through non-mandated means.

1.2 **Research Objectives**. The interconnectedness of the nation's critical infrastructure, coupled with the voluntary nature of cyber security measures creates great potential for negative externalities, or decisions that could result in costs to third-party stakeholders, related to national security in cyberspace. This research first examines the challenges the federal government faces in fostering private sector contributions to the nation's security that will reduce and ultimately remove these potential externalities. The dissertation first identifies the aspects of cyber security that should be considered a public good to strengthen national security for the United States. These aspects relate to the security of critical infrastructure and national security-related information systems. This research then identifies the challenges confronting the nation's security institutions as they attempt to secure critical IT and control systems enterprises to the level required to support national security. Having provided this foundation for understanding the public policy aspects of the issue, the research tests hypotheses related to both cyber security investment and the sharing of cyber security-related information.

In the area of cyber security investment, this research analyzes investment decisions and public policy options for cyber security in the defense industrial base using the Interdependent Security Investment (IDSI) model developed by Heal and Kunreuther (2003).[1] The IDSI model applies in situations where there is a threat of a catastrophic event occurring but the risk of it occurring depends on actions taken by others. Therefore, any agent's incentive to invest in defending against the risk depends on the actions of others also doing so (Heal and Kunreuther 2003). This analysis uses an empirically-based extension of the IDSI model that considers the underlying network characterizing interaction within the defense industry sector. I apply the IDSI model to an interaction network, based on actual contractual relationships, that is comprised of a sample of firms from the defense industrial base. This network topology is introduced to examine the impact of the network structure on tipping and cascading (as predicted by the model) in the security investment decisions of actors within the sample. This research tests the hypothesis that in a sector where the IDSI model accurately depicts the security investment decision, coordinated action directed at a small coalition can drive a system toward self-sustaining (non-regulated) investment at a level sufficient to foster system-wide, and ultimately, national security. I chose the defense industrial base sector for this portion of the research for two reasons. First, the inter-connectedness of the firms in this sector can be approximated by the contractual relationships

[1] Kunreuther and Heal originally used the acronym 'IDS' to stand for 'Inter-Dependent Security.' Since the cyber security field typically uses the acronym 'IDS' to stand for 'Intrusion Detection System,' I have added an 'I' to 'IDS' to capture the 'investment' component.

that are generated to develop major weapon systems programs. Second, because the knowledge required for designing the weapons represents a significant investment to the firm, successful theft of that information would be considered a catastrophic event, a major component of the model.

In the area of cyber security defense and response information-sharing, this research explores the assumption that private sector actors can be motivated to participate in the cooperative national security measures by empowering them to contribute to the development of those measures. The DHS authors of the NIPP theorize that a private sector actor can be motivated to participate in cyber security information-sharing when the private sector actor is given the opportunity (empowered) to shape the information-sharing regime (DHS 2006). I employ a case study approach to consider propositions related to information-sharing, with a focus on several firms in the electric power sector that have been actively engaged with DHS and the Department of Energy (DOE) on cyber security. This research tests the hypothesis that these firms contribute to the collaborative cyber security regimen because they and their industry organizations (e.g. sector coordinating council) were given the opportunity to shape the regimen through the development of the information-sharing protocols. The research also explores the potential for several alternate hypotheses that show different motivations to participate such as avoidance of further regulation and linkage through trusted third parties. I chose a different sector than the defense industrial base for this portion for two reasons. First, it demonstrates the diversity of the cyber security challenge between critical infrastructure sectors. Second, the diversity of both public and private stakeholders in the electric power sector leads to potentially more significant roles for the intermediate organizations such as the trade associations and the North American Electric Reliability Corporation (NERC).

1.3 **Contributions of the Research**. Because so many cyber security issues remain at a highly classified level or are proprietary, limited empirical analysis has been done in the area of cyber security. While a nascent field of cyber security economics has formed, there has been little academic research that addresses the national security aspects of cyber security beyond legal considerations. This research employs a mixed methods approach in an effort to bridge research previously done in the fields of economics and organizational behavior. The two parts of this research can stand alone as studies on each component of the cyber security problem in the nation's critical infrastructure, but the results of each part support the other. For example, as I will explain further in the conclusions chapter, insights into the motivation for sharing information obtained through the case study strengthen the results of the agent-based model. Interview responses from owner/operators support the different interaction spaces used in the model.

Although the analysis in this dissertation focuses on cyber security challenges confronted by the United States, the propositions contained herein are intended to be global. This work specifically takes a multidisciplinary approach to broaden the current cyber security research agenda and address this non-traditional but rapidly emerging security issue from multiple perspectives.

The defense industrial base was chosen for this research because there is a clear threat to the sector from cyber espionage conducted by competing firms, nation-states, or other malicious actors. However, the findings in this research should have public policy implications for addressing any situation in which the IDSI problem is occurring in an environment that approximates networked forms of interdependence. This might include other sectors of critical infrastructure such as electric utilities or finance. The most important contributions of this work relate to the difficulty of targeted intervention, or centrally coordinated behavior, to induce tipping in the security investment decision. As the results in Part II demonstrate, the interaction space of the actors within the system (e.g., the CI sector) can influence their perception of the threats to their systems and the investment decisions they should make. However, if sufficient numbers of actors choose to invest in adequate security measures, they may convince the entire system to follow suit and effectively improve their security posture and the security of the nation.

Regarding the case study analysis of private sector participation in the information-sharing network, a greater understanding of the factors that motivate participation by the private companies that comprise our nation's critical infrastructure will also have significant implications for national security. The most important result should be an understanding of how key actors in CI sectors can be motivated to share relevant and timely cyber security information. The results presented in Part III demonstrate that private sector actors are willing to share information if they can be assured that they can receive valuable cyber security information in return. As these information-sharing networks improve, the network should generate greater value for all participants, to include the national security community as it confronts a growing cyber component in diplomatic or military operations (Hare 2009). Nation-states are beginning to institutionalize tools being exploited by hackers and criminal elements so activities in cyber space may become critical components of negotiations and conflicts. Developed nations that rely extensively on cyberspace for their economic power and for controlling their infrastructure must begin to influence the use of cyber capabilities through international forums and prepare to respond to more concerted threats from the cyber domain. The international security community will be able to prepare for its future role more effectively when it more fully understands the homeland security challenge.

1.4 **Structure of Dissertation**. This dissertation is comprised of four parts. The current part will proceed with the presentation of cyber security as a national security issue in Chapter 2. The literature review in Chapter 3 concludes Part I. Part II contains the background, methodology, and results for the first research component, as regards the defense industrial base and cyber security investment. Part III moves to the background, methodology, and results for the second research component, the electric power sector case study. Part IV contains research conclusions and implications for public policy designed to motivate private sector contributions to the nation's security in cyberspace.

2 Cyber Security as an Issue of National Security

2.1 **Introduction**. In this section, I will present the theory of cyber security as an issue of national security. It is important to frame the issue in this light because there is still disagreement as to whether any additional policy measures are required to secure the nation in cyberspace (see, for example: Libicki 2009). The argument for considering cyber security as a national security issue proceeds from a discussion of securitization, or the process of making an issue one of national security, to the public good of national security. With this foundation, I place cyber security in the national security context and identify those aspects of security in cyberspace that are most important for national security. To begin my argument, I will define "cyberspace" as it relates to this research.

2.2 **What is cyberspace?** In recent years, the term "cyberspace" has become a popular component of security language. Although attacks on critical infrastructure through cyberspace were first highlighted extensively in Presidential Decision Directive 63 in 1998, the exact term was not actually used in that document. Instead, it spoke in terms of attacks on "cyber-based" systems (The White House 1998). By 2003, cyberspace became entrenched in the security language with the publication of the *National Strategy to Secure Cyberspace* released by the Bush administration in 2003. But it was not until the final year of the Bush administration that the term was fully defined by the federal government:

> The interdependent network of information technology infrastructures including the Internet, telecommunications networks, computer systems and embedded processors and controllers in critical industries (The White House 2008).

This definition, as contained within National Security Presidential Security Directive 54, makes an important point very clear—cyberspace is now considered larger than what has been commonly referred to as the Internet. Since the publication of William Gibson's (2004) book, the *Neuromancer,* pop culture has equated cyberspace with the virtual world of interaction and mass media made possible by a globally connected network. However this inter-connectivity is leveraged by much more than mass media, education, and other social media. Even the telecommunications industry itself is now transformed. For example, it is no longer possible to separate packet and circuit switched networks in any practical sense from a security, technology, or regulatory perspective. The backbones have converged in most developed nations and the convergence is extending further and further to the end user. We are now electronically connected, if not logically connected, from a child's laptop in Ghana to remote terminal units on control systems in critical infrastructure sectors in the United States and elsewhere. And these connections are not necessarily physical, cabled links; the control and data signals travel through space and across the airwaves. As stated by William Wulf (2007), of the National Academy of Engineering, “Best effort delivery is fundamental to the operations of the Internet.” Regardless of the path taken, the packets will find their way through eventually. The majority of critical industries now rely on this concept in many ways of which few in industry and government have a strong understanding.

It is also important to consider the relationship between cyberspace and information—the reason cyberspace exists. Cyberspace is not information or data, but the place where both are created, stored, modified, and exchanged. However, the environment and the content are clearly interwoven issues (Fahrenkrug 2010). Distinguishing between cyberspace and the information in cyberspace is important for assessing the actual vulnerabilities and developing cyber security policies. Whether it is the availability of the network or the availability of the information in the network that is critical drives much of the debate on cyber security. This relationship also drives differing perspectives on just how critical cyber security is and which components should be secured. For example, law enforcement agencies may stress the importance of securing identity and financial information whereas homeland securities agencies may focus on ensuring network availability.

2.3 **Cyber Security as an Issue of National Security**.[2] In this section, I will place cyber security in the greater field of security studies. To do so requires an assessment of the securitization process (explained below) and how cyber threats have been securitized by a diverse set of stakeholders. The goal of this section is to demonstrate that cyber threats can be considered national security issues and may therefore warrant public policy analysis and recommendations.

In his seminal article, "“National Security” as an Ambiguous Symbol,' Arnold Wolfers (1952) asserts that the decision to classify something as a threat to national security, and the measures that will be taken, are political decisions, not technological or legal. While most cyber security issues are considered highly technical, the issues must be made clear to non-technical policy-makers in order for them to enter the security agenda. Buzan et al (1997), writing half a century after Wolfers, delved more deeply into the process of moving a political agenda into the forefront of security; a process they call, "securitization." In other words, when an issue is presented as posing an existential threat (usually to the entire nation-state) that requires

[2] Portions of this section have been adapted with permission from a previously published article and presentation at the NATO Cooperative Cyber Defense Center of Excellence in June of this year (Hare 2010).

emergency measures (those that go beyond normal political actions), then it is being securitized (Buzan et al. 1997). Therefore, a threat, victim, and understanding of the threat to the victim are all required to engage in the process. In cyberspace, the threat agents can be criminals, hackers, terrorists, and nation-states.[3] The potential victims at risk from these threat vectors are also diverse. The threat actors may be in the business of stealing personal identities to commit fraud that, in the interconnected world of cyberspace, would make all individuals in a nation potential victims. Or the threat actors may be conducting industrial espionage. In the case of espionage, the direct victims are the target companies, but if the stolen information includes the plans for a new fighter aircraft, the taxpayer may again be considered a victim. In cases where the identified victim is the state and its institutions, the existential threat may be one of toppling the regime or one from sections of the country desiring autonomy. In cases where individual citizens face an existential risk to their welfare, either directly or through the loss of state institutions, a justification for public action can be made because national defense is considered a public good. Politicians are therefore motivated to securitize threats to individual citizens because they are charged to represent their constituents' interests and provide for public

[3] Further discussion on potential threat actors is contained in the Literature Review chapter.

goods.[4] Ultimately, several potential threats to many different stakeholders can exist in cyberspace. One can appreciate that a broad array of threat actors and broader consideration of potential victims can lead to a variety of securitization attempts.

The complexity of the various agendas can also be looked at from the perspective of government organizations. Federal agencies have differing perspectives on cyber security issues based on different responsibilities. For example, the foreign affairs department of a free society often champions freedom of information and freedom of expression. A free and uncensored cyberspace domain is a fundamental goal to further national interests from their perspective. An internal security department responsible for infrastructure and public safety is concerned about the security of national critical infrastructure. Therefore, their focus in cyberspace is resiliency and the availability of the interdependent networks for public and private use. The internal security agency is also concerned about the cyber security of critical infrastructure sectors that are linked through and dependent on the domain. An energy department has the same concerns, but they are clearly focused on the energy sector. Of primary importance to the energy department are the resiliency and electric generation and distribution and the security of the nuclear energy enterprise. National intelligence agencies

[4] And, of course, the politician will lose their office if they don't represent their constituents' interests.

have a much different focus. Intelligence agencies are energized by cyberspace because it allows them direct access to many more sources of information regarding threats to the nation without having to conduct risky operations on foreign soil. Law enforcement and commerce agencies are concerned primarily about the financial safety and identity protection of the nation's citizens in conducting commerce through the domain. Finally, a nation's military will be concerned about many factors related to cyberspace such as the availability of infrastructure to support military operations, winning the war of ideas in a conflict based on ideology, and the security of information related to national security and weapons programs.

Stakeholders in all the above areas and agencies may attempt to securitize these and other issues. However, when considering the idea of an existential threat and threats to national security, I argue that some issues and potential solutions should be prioritized above others. These threats may be real and currently impacting the nation's security, or there may only be an expectation thereof (Wolfers 1952). For example, the United States never fought a conventional conflict with the Soviet Union directly, but there was clearly a potential for conflict that led to many extraordinary or emergency national security measures. Although Buzan focuses on the push for emergency measures as an indication of securitization, many potential solutions to the above issues may amount to changing existing laws and political institutions.

2.4 **<u>The Public Good of National Cyber Security</u>.** To make the case for public policy, we first have to consider the public good of security. Using Buzan's concept of securitization introduced above, I will specify the public good of national security. For this work, it can be considered that state in which the public of a nation (the referent object) is not threatened by something, or someone, that poses an existential threat. To be a public good, no one in the population can be excluded from the secure state and the amount of security enjoyed by one person does not affect the level enjoyed by any others. Extending this concept to the public good of US national security, we have the following definition:

> The state of being in which the United States populace and governing institutions are not threatened by state or non-state actors that pose an existential threat to the people or the national institutions that are entrusted to ensure their security.

Conceivably, no US citizen is excluded from the opportunity to be secured to the same level (making the good non-excludable and non-rivalrous). The Department of Defense (DOD), Department of Homeland Security, and other federal and state institutions are primarily empowered to provide this public good. They do so through expenditures of taxes and being granted the legal authority to take actions against the existential threat actors such as foreign militaries and international terrorist organizations. From the standpoint of a

US citizen, the provision of this good by the government security agencies would not be considered a positive externality created by the government because the benefits are charged to the consumer of the good through taxes.

There are then primarily two ways in which this state of being is threatened by malicious actions in cyberspace. First, the nation can suffer an existential threat from attacks and infiltrations through cyberspace, by either state or organized non-state actors, against government, and other select information systems to gain knowledge of a national security value. Such activity is generally considered espionage. Potential targets include the systems of defense contractors developing major weapon systems.[5] Successful attacks would allow an adversary to counter a wide array of national defense measures and could justify extraordinary measures by the US government to thwart such attacks. Second, the nation can suffer an existential threat from attacks and infiltrations through cyberspace, by either state or organized non-state actors, against critical infrastructure systems (privately and publicly owned) to degrade or disrupt such systems. For example, attacks against such infrastructure sectors as energy, transportation, and in some cases, telecommunications, may endanger many

[5] On the other hand, individuals targeted for identity theft would not reach the threshold of national security.

lives directly or thwart attempts to defend the national interests.[6] Successful intrusions or attacks would also cause significant economic impact or loss of life, and could justify extraordinary measures to thwart their success. Placing these two criteria in the framework for national security developed above, we are presented with a definition for the public good of US national cyber security:

> The state of being in which the populace, governing institutions, and critical infrastructure are not threatened by
>
> - attacks and intrusions through cyberspace, by either state or organized non-state actors, against government and select other information systems to gain knowledge of a national security value
> - attacks and intrusions through cyberspace, by either state or organized non-state actors, against critical infrastructure systems (privately and publicly owned) to degrade or disrupt such systems creating a national security crisis

In general, the DOD and other federal and state institutions are *NOT* empowered (through budgetary and legal authority) to provide this public good.[7] If and when the good is provided, it is primarily provided by private actors who have little motivation to, or understanding how to, secure their systems with this goal in mind. Importantly these same actors are not specifically empowered to provide this good either through taxpayer provided funds or with specific legal authority. Therefore, the provision of national

[6] This criteria does not include attacks that could be adequately surmounted in sufficient time to prevent significant loss of life or to pose further risks to security (e.g., attacks against agriculture and monuments sectors)

[7] The partial exception to this rule would be the security of the information systems that are being used and managed by the federal government.

cyber security by these actors would be considered a positive externality in that it is not feasible to charge all the US citizens who would benefit. Since the majority of these actors do not seek to provide this public good, there is an existing, or potential, negative "security externality" that pertains to the state of being "cyber secure" as a nation. In other words, a security externality exists when a private firm undertakes an action, either directly or through omission, that creates a security vulnerability for the nation (Auerswald et al. 2006). I should also be clear that this state can never be fully attained. Even when all have invested as much as possible to secure their own and each other's systems, the complexity and dynamic nature of the problem at a national level means the risk will never reach zero. At best, we can work to attain a level of security at which the resiliency of the interdependent CI sectors is sufficient to successfully respond to concerted attacks without major cost to life and property.

In spite of the disincentives to act at a level that contributes to the public good, the federal government must rely on voluntary actions by the private firms in the CI sectors to secure their operations at a greater level than that from which they can individually benefit. As stated in the introduction, there are two important actions that should be conducted by all, regardless of the sector.

The first action firms must take is to invest in and implement strong cyber security measures in their IT and control system operations. The firms must invest to a level that accounts for their interconnectedness and considers the potential security externalities generated by insufficient investments. To support national security, this investment is especially important in such sectors as the defense industrial base, energy, and telecommunications. This research will explore cyber security investment in the defense industrial base to gain an understanding of the way the security investment decision can be dependent on the decisions of others in an interconnected environment.

The second major activity being promoted by the federal government is private sector participation in an information-sharing and response network. Not only does the defense against threats in cyberspace fall directly to the owner operators in each CI sector, but situational awareness of malicious activity cannot be developed without them. Without a network of radars with which to monitor the cyber frontiers, the nation's security institutions must rely on a network of public and private information sources. From the private sector's perspective, this network potentially provides valuable information on threats, vulnerabilities, and cyber security defenses. From the public sector's perspective, the network is of value to help data-fusion centers understand current attacks, current vulnerabilities, and defenses that have proven effective. Improved situational awareness also helps decision makers understand national-level response options. This research will explore the information-sharing process in a different CI sector, electric power generation and distribution. The diversity of this CI sector and the commitment of major organizations in the sector to national cyber security make it an important sector, one from which we can learn to improve public and private cooperation. Before presenting research related to these two issues, Part I will conclude with a literature review of works in research fields that will inform the current work.

3 Literature Review

3.1 **<u>Introduction</u>.** In Chapter 2, I developed the idea of national security in cyberspace to build the foundation for this dissertation research.[8] To articulate the issue more precisely, I employed concepts from the security studies field. As stated earlier, any effort to securitize a situation, whether in cyberspace or other physical domains, requires a threat agent, a victim, and an understanding of how the threat agent causes an existential threat to the victim (Buzan 1991, 115). In cyberspace, the threat agents can be criminals, hackers, terrorists, and nation-states. The greatest challenge is determining who is conducting the attack in order to understand motivations and response options. The targets of these actors are also diverse. The attacker may be in the business of stealing personal identities to commit fraud, conducting industrial espionage, engaging in cyber extortion of critical infrastructure owners, or preparing for and engaging in a major conflict accompanied by actions in cyberspace. Any analysis and body of policy recommendations that attempt to incorporate every possible combination of

[8] The majority of the literature for this dissertation was adapted from the supporting Fields Statement.

these malicious actors and their attack motivations would be hard pressed to escape the trap of ambiguity. To summarize from Chapter 2, the national security component of the cyber security issue addressed in this research will entail the following:

> Attacks and infiltrations through cyberspace by either state or organized non-state actors against government and critical infrastructure systems (privately and publicly owned) to gain knowledge of a national security value and/or attempt to degrade and disrupt such systems.

National security is primarily about threats to the existence of a nation-state (Buzan et al. 1997). Obtaining knowledge of value to national security can create an existential threat by allowing potential adversaries to gain the knowledge to develop effective counter-measures to a nation's advanced military and other defenses. In addition, cyber attacks that degrade the ability to command and control national security assets and attacks that disrupt critical infrastructure have direct implications for national security. This infrastructure may be civilian, military, or both. In the United States, for example, the Department of Defense relies heavily on the nation's public and private cyber infrastructure backbone for communications purposes (Wilson 2004). Although the concept of national security in cyberspace is limited by the above convention, the academic fields that inform research in the area of national security for cyberspace are nonetheless diverse.

The following three fields are central to providing a theoretical framework for the research area described above: the economics of information security, cyber conflict, and inter-organizational behavior. Literature in each field is presented in the sections that follow. In the next section, I explore the field of economics of information security. As the preponderance of actions to secure the nation in cyberspace must be undertaken by private actors, their perspective, a necessarily economic one, must be considered first. This section builds a theoretical framework for the motivations and decisions of private and, to a degree, public actors to invest in the private and public good of security measures. The second section moves to a focus on the threat actors and the potential national responses to improve security including roles for the national security community. Because so many current issues are still of a highly classified nature, limited empirical analysis, and therefore limited quantitative analysis, has been done in this area. The majority of works discuss the respective roles of national actors and the legal frameworks within which they would act. The final theoretical field of significance relates to organizational behavior. As will be highlighted throughout this review, there are a multitude of organizations that must work together voluntarily to address cyber security. Therefore, it is helpful to understand both their internal workings and their relationships with each other. The human dynamics that drive these interactions often play a significant role compared to the purely economic aspects of security investment and cooperation decisions.

3.2 **Economics of Information Security**. Though still a relatively small field, the economic dimension of information security has begun to grow as the nation has come to rely increasingly on information systems to store a variety of important information (Garcia and Horowitz 2007). Businesses and public organizations have recognized the great cost savings that come from automating the storage and distribution of their most valuable assets—information. But they have also learned that this automation has created potential vulnerabilities and that some level of security must be implemented. Even if the value of their security measures is not always clear, firms must implement something if only to reduce their liability from potential losses.

A reason for why this field remains small can be discerned from the very definition of "information security" which is actually defined in US legal code. Specifically, information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, in order to provide; integrity (guarding against improper information modification or destruction), confidentiality (preserving authorized restrictions on access and disclosure), and availability (timely and reliable access to and use of information).[9] Necessarily, a full appreciation for these fairly technical concepts, and the actions that must be taken to ensure security of information, requires a working understanding of the software and hardware components of information systems. Both hardware and software engineering have become increasingly technologically complex. Therefore, most researchers in this field began their information security studies as computer scientists. These researchers have a detailed understanding of the measures that must be built into systems and implemented by professionals responsible for the affected networks and data servers. Along with this expertise, they have begun to expand into management and economic aspects of the security investment decisions. On the other hand, relatively fewer economists and management professionals have chosen to move into the information security field from direction of the social sciences. According to Jeffrey Hunker (2002), dean of the Carnegie Mellon Heinz School, "Research into these questions [interdependent network security] spans both technological and social/decision science realms. Few if any serious researchers have the breadth of knowledge across these disciplines to begin to creatively integrate new perspectives" (pg 709). That said, many seminal works in the field of economics inform the economic aspects of information security. As with any investment decision, the

[9] 44 U.S.C. § 3542.

economics of information security most often focuses on the cost/benefit analysis of investing in one opportunity given the alternatives for the investment in other business areas such as research and development. This investment decision can be theoretically quantified even if empirical data to support theories is lacking. The more challenging aspects come with consideration of the public good and externality components of information and cyber security. While it is difficult to obtain the appropriate amount of information to make an informed investment decision from the business perspective, it is even more difficult to quantify the national security aspects of cyber security that are considered public goods, such as the privacy of customers' information and the security of critical infrastructure against a nation-state attack. The works reviewed in the rest of this section range from the cyber security investment decisions internal to firms to fostering investment at a level that reduces negative externalities and supports the greater public good of national security.

3.2.1 **The Cyber Security Investment Decision**. As stated previously, quantitative models have been developed to depict the cyber security investment decision from the perspective of an economic entity such as a corporation. Such entities employ an information system network containing either important financial or personnel data, the disclosure of which would have economic consequences. A number of researchers have taken this mathematical approach in their work. In *Managing Cybersecurity Resources*, Lawrence Gorden and Martin Loeb (2006) provide a straight-forward cost-benefit analytical framework for a firm's cyber security investment decision. They present the cyber security investment decision problem using standard accounting concepts such as dividing expenditures into operating costs and capital investments. They further classify the net benefits by their net present value and rates of return in an effort to equate the decision to standard financial planning as much as possible (Gordon and Loeb 2006). The benefit of using commonly accepted techniques is that the financial planners of a company can try to compare investment decision "apples with apples." Unless the people in a firm who are responsible for information security can articulate the benefits of the investment in terms that are understandable to the firms budget personnel and financial decision-makers, they do not stand much of a chance of receiving support for their agenda. The drawback to such a simple model, however, lies in the security personnel's ability to measure the true costs of a failure to secure the information. While the direct cost of security measures can be quantified in dollar terms (e.g., the cost of software and wages), the cost of a failure to secure is probabilistic. Gordon and Loeb (2004) recognize this and have presented models to account for the monetary loss to a firm from a successful security breach given the probability of such breach. In simple terms, the potential loss equals the probability of a successful attack times the total possible loss. However, the vulnerability changes with the investment in security. How exactly it changes is not directly measurable, but Gordon and Loeb provide a potential model for the relationship between investment, probability of attack, and potential loss. According to this analysis, an optimal level of investment can be determined mathematically if one ignores the potentially competing requirements of the components of information security (e.g., authenticity, confidentiality, and availability). This particular model in itself is not overly complex, but no empirical work has been done to test its validity, and coupling it with the basic cost-benefit analysis generates a more complex case to be argued before the budget office.

Several other researchers continue the cost-benefit line of inquiry but attempt to resolve the challenges of articulating many of the potential costs of cyber security. Farahmand et al. (2004) take a further look at articulating the cost of an information security incident. They identify three categories of loss—productivity, revenue, financial performance (to include stock value loss resulting from damaged reputation)—and other expenses such as overtime and equipment rental to remediate damages (Farahmand et al. 2004). While these authors do not present a formal model to quantify these costs, they do provide more data points for an investor to add rigor to their analysis and to argue the significance of their investment given the range of threats and potential losses a company may face. Huseyin Cavusoglu et al. (2004) provide a fairly technical view of how potential investments can be compared to each other by considering a combination of attack vectors and techniques. Such an evaluation is an equally challenging aspect of the cyber security investment. Not only is it difficult to justify an investment in cyber security compared to one in, marketing, it can also be very difficult to determine which cyber security investment would be the most cost-effective. This model accounts for the combination of firewalls, intrusion-detection systems, and monitoring devices that must be employed in concert for a security system to be effective (Cavusoglu, Mishra, and Raghunathan 2004). One benefit of their approach is that it also accounts for the fact that the attacker is a calculating entity that plans their attack based on the defenses it confronts. Incorporating this component in a model is important since no security system can be considered to be static or "non-adaptive." Cyber defensive measures are always employed against a calculating threat. In his recent article on cyber security investment, Kjell Hausken (2006) presents arguably the most comprehensive investment model, from a neo-classical perspective, in his recent article on cyber security investments. Hausken not only considers the attackers decision making, he attempts to account for the interdependence of the actors employing cyber security measures, and the income and substitution effects as they try to maximize their overall utility.

This author does an excellent job of articulating the impact and inter-related nature of several investment variables on each firm's investment decisions, including how one firms investment will change the potential risk of attack for another firm. However, one can imagine how complex the calculations become as the model becomes increasingly inclusive. Not only is it difficult to imagine that any of the calculations would be explicitly conducted by a firm, but the amount of empirical information required to solve the equations leads one to question the model's ultimate value. Nonetheless, it provides a goal to strive for in future empirical research.

3.2.2 **Information in the Cyber Security Market**. As identified earlier, one of the largest challenges to researching cyber security is determining the true value of costs and benefits. Identifying what costs should be considered is only the first step in estimating the accurate values for such costs. This concern is where landmark works in the field of economics can be of value to the cyber security field. In "The Use of Knowledge in Society," Hayek (1945) articulates the fundamental issues regarding the consideration of any economic endeavor from the traditional neo-classical perspective, which requires the potentially unrealistic expectation that the actors have a common knowledge of market conditions. Admittedly, Hayek was most critical of centrally-planned economic structures, but he was also highly critical of mathematical economics that assume an unrealistic knowledge of market conditions (Hayek 1945). To Hayek, the central goal of economic research endeavors was improving knowledge in the system instead of assuming it was all there. In his work, he spoke of markets where information could theoretically be made visible to all participants. Yet, we seem to be ignoring Hayek's warnings and marching forward with detailed economic models in a research area where empirical data and true benefit-cost knowledge is virtually impossible to obtain even on a micro level.

Although equally challenging to obtain, knowledge of the investment decisions of other entities is of particular importance. The fact that the investment decision is not visible to others influences the behavior of all actors in the system. Schelling (1978) illustrates this in his discussion of binary choices. As he states, "If people need to know how others are choosing, to make their own choices, it will matter whether or not they can find out what everybody is doing" (pg 215). The classic example of this issue is the Prisoner's Dilemma. If the prisoners could coordinate a non-response, they could walk free. But since they can't coordinate their decisions, each assumes the other will rat and tries to be the first to plea bargain. Schelling provides several potentially insightful scenarios and identifies the parameters of importance. His ability to present such binary choices in a straight-forward manner with limited mathematics makes them very accessible for the research and enhances their explanatory power. As will be discussed in more detail below, this scenario relates to cyber security within an interconnected system (e.g., power production companies).

Several authors have acknowledged the challenges of improving information-sharing on information security and have catalogued the main impediments to such cooperation. Among them, Carl Landwehr (2004) provides an insightful history of the US Department of Defense (DOD) attempts to enforce standards in the security components of information systems. In the early days, the DOD tried to build all necessary equipment either internally or to government specifications from top to bottom (Landwehr 2004). That was eventually determined to be cost-prohibitive and they then turned to commercial systems that would ostensibly meet minimum security requirements. But even with the publication of such specifications, evaluating security systems was easier said than done. According to Landwehr (2004),

> The properties are not only difficult to specify and quantify, they are time consuming to evaluate. Though asymmetric information may be a factor in this market, in that a seller may know more about the security properties of his product than the buyer can, in many cases even the vendor lacks full knowledge of his product (pg 162).

This challenge leaves the firm's security professional with yet another trade-off. They may forsake the latest, most productive systems for older, more secure models that have fewer features in order to achieve the desired level of security against the already difficult to quantify threat (Landwehr 2004).

However, management may have little interest in an investment in older IT that would put the firm at a productivity disadvantage to its competitors.

Other researchers have also identified this challenge and are addressing information-sharing and the amount of knowledge available to actors making cyber security investment decisions. Researchers Esther Gal-Or and Anindya Ghose (2004) explore the issues with sharing information between competing firms and with a federal government entity encharged to monitor and support the private sector's information security efforts. Gal-Or and Ghose use a game-theoretic construct to show how industry characteristics affect their incentives to share information and how this action can affect profits. Their research provides several encouraging results. According to their simple model of a two-firm market, a higher level of information-sharing related to security breaches by one company leads to a higher level of information-sharing by the other, and a potentially higher level of technology investment by both (Gal-Or and Ghose 2004, pg 102). It is important to note here that the sharing must occur between the two companies, not just with the federal agency. Otherwise, the efforts of each firm are not transparent and have no effect on the other firm. In reality, the federal agency may serve as the conduit. However, the agency may be required to mask a firm's identity to facilitate their sharing of information. This action is an important step in overcoming one of the major disincentives to share information—the concern that disclosing a security breach will lead to a claim of liability on the part of the firm.[10] Unfortunately few other researchers in this field have provided useful models for improving the sharing of information both on the level of a firm's investment and the successful or unsuccessful attacks against their systems. One must look to the other fields that will be presented in this review, specifically inter-organizational behavior for more consideration on how to improve the flow of information related to cyber attacks.

3.2.3 **Security Externalities and the Public Good of National Cyber Security**. To this point, I have focused on the concerns facing a firm and their investment decision from their own perspective and for their own interests. However, as has been noted, there is a significant potential for a negative externality to occur when a firm has underinvested in cyber security. This is especially important when considering the sectors of importance for this work—those comprising the nation's critical infrastructure. The interdependent nature of many of these sectors, such as finance, electricity, emergency services, telecommunications, and the defense industrial base has been a cause of growing concern since the Clinton

[10] This concern about potential liability demonstrates one of the fundamental differences between an attack on a facility from the air and one through cyberspace. If a foreign country bombed a hydro-electric dam, the US military would probably be found at fault. No one would look to the utility owner to assume any liability for the successful attack. However, if the attack came through cyberspace and had the same effect in shutting down power generation, the first entity to be held liable would be the utility. The U.S. military would not even enter the discussion until considerations for retaliation.

administration (Kathi Brown 2006). All these sectors are not only closely tied between firms in their sector, but in many cases, the sectors themselves are greatly interconnected, especially through cyberspace. Several authors raise this issue in their work. In fact, it is a major theme of the book, *Seeds of Disaster, Roots of Response*. The editors of this book introduce the concept "security externality" and define it as, " a private firm undertaking an action that creates a vulnerability (or possibly an uncompensated benefit) elsewhere in the economy (Auerswald et al. 2006, 9)." The editors then assert that a goal of public policy should be to provide the necessary incentives to private sector actors to invest adequately in security or otherwise reduce the potential externality (Auerswald et al. 2006). Lewis Branscomb (2006), in his overview of the book, suggests that, "all elements of society … are both subject to expanded risk and also bear growing responsibility for its mitigation" (pg. 19). Branscomb states that the lack of clear accountability for addressing the threats that arise from security externalities contributes to the "seeds of disaster." In his introduction to the book's section on securing networks, Philip Auerswald (2006) summarizes the ideas regarding coordination of actions of the respective firms. To a degree, the under-investment is a form of the tragedy of the commons. In other words, both horizontally and vertically linked infrastructure networks suffer from an "over use" of reliance on the current absence of a failure of the system. If any one actor cannot keep the failure from occurring (akin to overgrazing on the commons), they will continue to press ahead with an under-investment so as not to potentially waste the dollars at the required level of security (Auerswald 2006, 161). Putting the problem in this perspective helps future researchers frame their empirical work and look to previously useful policy solutions to address these issues. Contributors to this book provide numerous examples of different scenarios where such externalities are prominent and give recommendations for measures that can be enacted to reduce these externalities. For example, Heal et al (2006), while not presenting any empirical evidence that their potential policy recommendations would be effective, nevertheless present a useful menu of policy proposals that could aid policy analysts and researchers. They discuss the ideas of encouraging trade associations to take a greater role, enticing key or leading firms to set examples, requiring third-party auditing of security systems, and establishing requirements for cyber security insurance. Finally, Todd LaPorte (2006) explores an alternative solution to ensuring a greater level of security. He stresses six organizational actions that can be taken to improve security through resilience. According to LaPorte, resilience is obtained through building a professional workforce, making the organization adaptive, and encouraging continual learning of threats and response actions among other things. In the end, nothing short of political leadership and continuous attention will be required to ensure the cross organizational interaction necessary to implement these solutions (La Porte 2006). The implication is that leaving the private sector to pursue such agendas on their own will not guarantee adequate devotion to an acceptable reduction in national risk.

Several other researchers are addressing this important issue of interconnectedness and interdependence. With the rise of international terrorism and its ability to target both public infrastructure and private assets, several authors have identified the potential for cascading effects both horizontally and vertically through industry. Yosef Sheffi (2005), in his book, *The Resilient Enterprise,* suggests that supply chains collaborate on security in order to ensure the resilience of the chain and mitigate the impacts of potential disruptions. Sheffi highlights the vulnerability of container ports coupled with their criticality to international supply chains. These facilities are clearly the nexus of several critical infrastructures in our nation. As Sheffi points out, awareness of this risk has led to several public-private collaborations to raise the security level at these facilities, to include the Business Anti-Smuggling Campaign, the Customs-Trade Partnership against Terrorism Program, and several others (Sheffi 2005, pg 147).

One of the most versatile economics tools for demonstrating horizontal and vertical linkages on an economy-wide scale is the Leontief input-output model. By placing an entire economy (local, regional, or national) within a matrix that demonstrates the flows between the sectors, a researcher can analyze how shocks to any one sector may impact another.[11] While the framework has normally been used to show economic inter-connections (flows of products and labor), Yacov Haimes and Clyde Chittester (2005) have taken the novel approach of adapting this methodology to demonstrate the interconnected nature of critical infrastructures control systems using an operational risk perspective. These researchers employ a metric called "percentage of inoperability" which reflects the "risk of inoperability resulting from complexity and intra- and interconnectedness (pg 5)." Once they have identified the interdependency matrix, they attempt to demonstrate the risk of inoperability that spreads throughout the intra- and inter-connected critical infrastructure systems. This model can be useful in that it allows planners to estimate the system-wide impact of an attack in dollar terms. It also provides a potential metric for assessing the value of risk management measures at a level that more closely approximates the provision of the public good. At a minimum, this model clearly establishes the tangible impact of interdependence and interconnectivity—two important aspects of the cyber security issue.

[11] Historically, this tool has been used to plan economic development and contractions by showing how, for example, the building of a new manufacturing facility will lead to an increased demand in the food sector that may lead to an increase for demand in the used car sector (more cars for pizza deliverers) and so on.

3.2.4 **The Potential for Under-investing in Cyber Security.** Several authors have presented the case for underinvestment from the public's perspective in a quantitative manner. Jack Hirshleifer (1983) presented an interesting perspective when he compared three scenarios for the voluntary provision of a public good related to security, the best-shot, weakest link, and summation of effort. In his article, he used the analogy of several landowners on an island requiring dikes around their plots so as not to suffer floods from the ocean.[12] Hirshleifer was able to show mathematically and graphically what the efficient amount of provision is for each situation of effort. He demonstrated that in the case of summation of effort, one can expect a large underprovision of actual effort, especially as the group size increases (Hirshleifer 1983). In addition, when the best-shot is all that is required, most others will free-ride, and when the weakest-link is the most important, the group will work together closely to ensure a minimum level of effort (Hirshleifer 1983). To a varying degree all aspects can be present in a cyber security scenario.[13] Although it is difficult to create an empirical model to

[12] Varian (2004) uses a clearer example of city defenders. In some situations, the weakest link may cause the defenses to crack, in others, a sum of all the efforts may hold off the attackers, in yet others, if a strong defender can sally forth and repulse an attack, the best shot may win.

[13] For example, consider the efforts to defend a corporate LAN. If any one employee clicks on the phishing scam, their account can be compromised and an intruder may access critical files across the company. Or perhaps, all the employees are conscious of the threat from phishing and the company has a defense-in depth approach, with multiple security features. All employed together serve to repel a persistent threat. Finally, imagine a scenario where several corporations are under a denial of service attack and one of the defenders alters the attacking code and sends it back to the controller. As long as one packet successfully arrives and neutralizes the attack (the best-shot) all the victims will be saved from the onslaught.

demonstrate the amount of "effort" that is being employed at a national level to provide for cyber security, this work does support the argument that, other factors being equal, we can expect that there is a substantial underinvestment. In fact, given that it is difficult for each actor to observe their level of contribution to the public good, or even to quantify a potential level that they or anyone else may observe, the disincentive to invest to a level of a public good, may be even stronger. Hal Varian (2004) took Hershleifer's work a few steps further by exploring the possibilities of Nash equilibria in two-person constructs and considering the adaptations of a potential adversary. Varian also took an important step by introducing measures in his model to reduce the potential for free-riding and under-investing on an individual level. For example, if a fine could be established that equates to the cost imposed on agents who are not free-riding, it would effectively induce the socially optimal level of effort depending on the type of effort required (i.e., summation instead of weakest link) (Varian 2004). Varian's work took this line of research closer to applicability within cyber security as his focus was on system assurance specifically. Yet a further step was taken by Alfredo Garcia and Barry Horowitz (2007) in their paper, "The Potential for Underinvestment in Internet Security: Implications for Regulatory Policy." Their research showed that there is clear potential for a socially sub-optimal level of investment in security by Internet Security

Providers (ISP) as the social value from consumption (of bandwidth) greatly exceeds the revenue at stake for the service providers (Garcia and Horowitz 2007). The gap increases with the size of the market and competition between ISPs. Although their results suggest the introduction of a regulatory policy, the authors are not optimistic about one's success for a variety of reasons. Garcia and Horowitz identify problems with the ability to accurately estimate the probability and impact of an attack (to what level should security be regulated), the adaptation of attackers to new techniques (maintenance of an effective regulatory regime over time), and industrial readiness (one-size-fits-none regulation). In a related article by Jean Camp and Cathy Walfram (2004), the authors present a novel solution for addressing these shortfalls by establishing a market for vulnerabilities (akin to a market for polluting rights). However the fact that the market price would be determined by the expected severity of damage from vulnerabilities and the cost of correcting or working around the vulnerabilities does not get us past the first problem with regulation; establishing the expected loss (not as easy as measuring the amount of pollutants in the air). Admittedly, this article does not focus on a potential failure that would necessarily lead to a national security concern, but it would be possible to extend the consideration beyond e-commerce and general Internet availability. Granted, a full disruption or even large-scale, lengthy degradation of the public Internet is not a very plausible scenario. However, the economic and other social or public costs associated with such an event would clearly justify the added investment in security and could be incorporated within this model to enhance its results.

Boehme and Moore (2009) consider that under-investing may be a rational action, but not necessarily an attempt to free-ride. They suggest that in an adaptive environment, it would make sense for the firm to wait for intrusion attempts to identify where the true weakest link is, then dedicate resources appropriately. If one expects the attackers to operate strategically and migrate to the weakest link in a defense, it would make sense for the defender to adapt strategically as well (Boehme and Moore 2009). Adapting to the identification of the weakest link over time helps the defender overcome shortcomings in their knowledge base and invest more wisely. This could increase a firm's general incentive to invest.

3.2.5 **Additional Ideas on Regulation**. While most of the researchers surveyed to this point offer some suggestions for correcting for under-investment through various forms of regulation, they often stop short of detailed proposals. Most concerted research on regulatory solutions related specifically to cyber security, has focused on the need to direct that more secure systems be built (better standards in IT components), and to promote a larger market for cyber security insurance. For example, a frequent advocate for inducing IT system producers to make more secure systems is Ross Anderson from Oxford. In a paper he co-authored with Tyler Moore (2006), Anderson points out that "insecure software dominates the market for the simple reason that most users cannot distinguish it from secure software … software developers are not compensated for costly efforts to strengthen their code" (pg 2). His main recommendation to address this market-failure is to advocate the introduction of some type of vulnerability market and he provides a review of several alternatives. The main draw back of any such solution is the introduction of an incentive for uncovering flaws that might otherwise go unnoticed (Anderson and Moore 2006). This development becomes a problem if the main users of this information are malicious actors and those who need to be protected fail to act accordingly. Several other researchers have looked at various aspects of the cyber insurance market. Recently, Walter Baer and Andrew Parkinson (2007) conducted a comprehensive review of the issues surrounding the cyber insurance market and the state of current research. They highlighted a long list of barriers to the expansion of insurance into the information security realm, such as the ever-present information asymmetry. According to these authors, government actions to assign liability for IT security breaches, and contractual requirements that government contractors carry cyber liability insurance, are two proposals that should be considered and researched further (Baer and Parkinson 2007). Critical analysis of either these or other components of the industry have been left to other researchers. One complex analysis using computer simulations to identify insurance market equilibria was undertaken by Rainer Böhme and Gaurav Kataria (2006). Their work sought to shed light on the problem of event correlation, both internal to an organization and globally, due to the trend toward standardized products. According to their model, it can be expected that insurers will be reluctant to insure for events or to insure certain companies that have exposed themselves to the possibility of suffering damage due to an event that creates wide-spread damage across the Internet (most likely due to their over-reliance on standardized products) (Böhme and Kataria 2006). Their proposal to overcome this problem is to encourage product diversification, but market forces will continue to make such proposals largely unattractive until the threat becomes much more tangible for the average company. In fact, Boehme teamed with Galina Schwartz (2010) several years later to assess progress in the cyber insurance field. They have found that there is still a wide gap between the potential for employing insurance mechanisms and the current size of the market. A study by Jean Bolot and Marc LeLarge (2008) demonstrated the potential positive effects of inducing the adoption of insurance in a networked environment. Combining game-theoretic analysis of insurance investment and interdependent security investments with consideration of network topology, these authors showed how the adoption of insurance can theoretically tip the collection of actors in an industry toward a Nash equilibrium of full investing (Bolot and Lelarge 2008). One interesting preliminary finding they observed when introducing a star network topology to influence the decision process is that the central actors had a stronger disincentive to invest while the actors on the nodes tended to follow the lead of the central actors (Bolot and Lelarge 2008). They remarked that a precise analysis of this phenomenon would be left to future researchers.[14] Regardless, this is one of the few works that has taken a truly multi-disciplinary look at the issues of improving security investments in the cyber realm.

Although the above-described scholarly works all consider the implications and probability for public policy to address the negative security externalities created by under-investments in cyber security, the fact remains that the actors will remain self-regulated for the foreseeable future. Therefore, it is useful to consider three significant studies on self-regulation in critical infrastructure industries to gauge how successful we can expect self-regulation to be. Anil Gupta and Lawrence Lad (1983a) compare several

[14] I include this remark because I observed the same phenomenon via a very different route. I used an agent-based model and observed this tendency while the agents were making their investment decisions. I would be hard-pressed to follow their mathematical proof of the event, but their explanation of why it happens is fairly similar to one proposed in Part II of this dissertation. They, however, did not have the benefit of seeing it happen in the model. They could only predict it.

alternatives regarding regulatory structures, both from self-regulating and governmental regulating perspectives. They then present seven propositions for situations in which they assert one or another form of regulatory structure may be more effective. Because of the diverse nature of each of the sectors comprising the nation's critical infrastructure, at least the following three have potential applicability to the current research problem:

> Proposition 2: Industry self-regulation is more likely in situations in which the externally imposed costs from not undertaking such self-regulation would be greater than the cost of undertaking such self-regulation.
>
> Proposition 3: The existence of an industry- wide decision making system (such as a trade association) increases the probability of industry self-regulation.
> 3A: Industry self-regulation is more likely when it requires coordination among firms on an intra-industry rather than on an inter-industry basis.
> 3B: The more fragmented an industry, the less the likelihood of industry self-regulation.
>
> Proposition 4: If standard-setting committees/task forces are comprised largely of full-time employees of the industry association rather than of member firms on part-time assignment, then the proposed standards are likely to be perceived by neutral observers as more equitable in terms of their impact on the member firms (Anil K Gupta and Lad 1983a, 420-422).

Both proposition 3 and 4 suggest research that focuses on trade associations and their role in supporting self-regulation. In addition to trade organizations, several of the sectors comprising critical infrastructure have Information-sharing & Analysis Centers (ISAC). These centers are an additional source of expertise to support the development of industry-wide standards. Neil Gunningham and Joseph Rees (1997) are proponents of self-regulation and feel that too much emphasis is placed on trying to regulate corporate action through governmental actions. According to these authors, building transparency into corporate processes is what is required to increase "the likelihood of being called to account for one's industrial processes" (Gunningham and Rees 1997, 386). Finally, Andrew King and Michael Lenox (2000) conducted a highly cited analysis of self-regulation in the chemical industry following the Bhopal incident in 1984. Through their case study, they sought to analyze the impact of a industry self-regulation program by reviewing the environmental safety programs of chemical firms before and after the introduction of the program. In general, their results suggested that the firms were motivated to join the program, however the firm's environmental records did not show significant improvement after doing so (King and Lenox 2000).

One of the important aspects of self-regulation regarding cyber security is the fact that security measures, unlike physical security, are largely invisible to the outside observer or even to other firms in the industry. This factor will most likely contribute to the continued failure of self-regulation to counter the generation of negative security externalities due to under-investment. However, not all nations follow the market-based, self-regulation approach in this area. A recent work by an Israeli researcher, Dan

Assaf (2008) provides an insightful comparison between the United States and Israeli approaches to critical infrastructure protection. While several previous authors have noted that the US relies on the private actors in all the critical infrastructure sectors to regulate their own behavior, Assaf places Israel at the opposite end of the regulatory spectrum. According to this researcher, the Israel model is decidedly interventionist with "law and hierarchical control as its cornerstone" (pg 8). Clearly, the immediate, physical threats faced by Israel are more tangible and visible than similar threats to critical US infrastructure. However, in cyberspace, there is no need for a potential adversary to be physically near to pose a credible threat. A state can be threatened from anywhere in the world against any component that is directly, or indirectly, connected to the commercially available Internet. At a minimum, there may be some lessons to be learned from the Israeli model to assess the potential economic impacts of a more regulatory approach to security in the domain.

3.3 **Cyber Conflict and National Security.** The limited number of researchers in the field of cyber conflict have taken a more qualitative approach to their research than economics researchers have to theirs, but their agendas are as diverse as those researching the economic aspects of cyber security. As with any issue that advocates seek to add to the national security agenda, there is a need to identify the clear threats, vulnerable targets, and the risks these threats pose to a nation's level of security. To inform the national cyber security debate, cyber conflict researchers have identified a wide collection of potential threats against cyber systems. One of the difficulties in distinguishing the different threat actors is that they mostly act anonymously, while their tools and techniques are very similar. Therefore, most researchers rely on motives and targets to discern how the actors may be categorized. Since the field is not dominated by logical positivist, or policy science, thinkers, cyber security theorists tend to be normative or to discuss more in-depth, prescriptive approaches to securing the domain. For example, a number of books have been written that present a strategy for how a nation can become a "cyber power." What is interesting is that the various authors seem to take a fundamentally different approach to achieving this goal.

3.3.1 **Cyber Threat Actors.** An important characteristic of conflict in cyberspace is that the threat to a nation's security can come from both well-financed and well-trained nation-state actors, as well as non-state actors with significantly fewer monetary resources. Since a simple lap-top computer can be employed as a weapon, virtually anyone can "fire" one in anger. In addition, the actor can do so with little physical risk to their person or even risk of being discovered as the perpetrator of the offensive act. As a result, several categories of threats must be considered. Beyond the ever-present prank hackers, criminal hackers, and insider threats, most authors have grouped the remaining malicious actors into the general categories of “hacktivists,” cyberterrorists, and state-sponsored or other non-state actors with the ability to conduct a strategic level of warfare in cyberspace. Dorothy Denning (2001), a prominent cyber security researcher with the Naval Postgraduate School, recently reviewed the potential threats posed by a wide selection of characters. Denning characterizes hacktivism as hacking websites as a form of activism. The activity is not intended to cause serious damage, but merely to cause disruptions in order to promote awareness of an issue (Denning 2001). With this in mind, the ethics of a hacktivist would suggest that such actors do not pose a threat to a nation’s security. The other category of non-state sponsored actor that is often the focus of concern in the popular press is terrorists. Denning also explores the idea of ‘cyberterrorism,’ or the convergence of cyberspace and terrorism. Examples abound and boundaries can be fuzzy between what could be considered hacking, criminal activity and terrorism. However, there have been no recorded acts of cyberterror to date. The threat of cyberterror is lowered by two simple facts; it is difficult to get “the CNN effect” and instill fear in the minds of ordinary citizens through an act of cyberterror; and if that effect can best be achieved relatively easy with a bomb attack, why bother to change tactics (Denning 2001)? Despite periodic alarms to the contrary, most other authors support

Denning's view (see Schneier 2003; Gorman 2006). For example, Irv Lachow (2009), at the National Defense University, analyzed the skills and training time, 6 to 10 years, required for a terrorist organization to conduct the type of cyber attack that would have the impact of an indiscriminate bombing. Considering the investment required, it would seem much more cost-effective to continue pursuing the physical attack route, especially while the supply of suicide-bombers appears endless.

As stated previously, the main threat this research will focus on is the last category of state-sponsored threats or other non-state actors who would attack with the goal of purposefully damaging critical US infrastructure or of conducting extensive espionage to gather national security related information. These types of activities require the capability to conduct a strategic information war with which to achieve such goals such as damaging a national economy, or delaying a nation's response to a physical attack (Rattray 2001). According to Dr. Greg Rattray (2001), formerly of the US Department of Defense, developing the capability to conduct strategic information warfare requires the knowledge and understanding for conducting hacking and other criminal activities, but also requires an understanding of how an attack will disrupt the operations of the targeted entity. These skills also require a strategic understand of the significance of information that may be stolen through cyberspace. A nation-state foe is less concerned about someone's social security numbers than they are with finding an adversary's defense plans and critical technologies. These factors suggest that an offensive strike from nation-states or other non-state actors will be very situation dependent. In other words, a cyber attack that was not coordinated to achieve a specific, national objective would not be worth the risk of discovery of the means, or the source of an attack.

Unfortunately, as the speculative nature of reporting in the popular press has shown, the ability of researchers to analyze the occurrences and effectiveness of nation-state-level attacks in cyberspace is severely limited. Researchers are mostly reliant on the writings of foreign military authors to discern capability and intent. In his book *Cyber Silhouettes,* Timothy Thomas (2005), of the US Army's Foreign Military Studies Office, provides an assessment of the cyber warfare intentions of both the Russian and Chinese militaries. While he provides no insight into their actual capability, he does explain how their military doctrines embraces the idea of fighting in cyberspace and the importance they place on developing an effective fighting force to operate in that domain. Thomas explains that both countries consider information attacks on their adversaries to be integral parts of their strategy. What better way to reach a target with information, or deny someone information, than through cyberspace? Additionally, Thomas cites frequent cross-straits battles in cyberspace between China and Taiwan as the former attempts to demonstrate its control over the latter in all domains. Chris Wu (2006), a contributor to a 2006 collection on Information Warfare (IW) articles, agrees with Thomas but caveats the significance of Chinese military theory writings by suggesting that, as recently as 2004, China lacked the indigenous hardware and software development skills to carry out the strategy. Now that China has taken a leading role in the development of Microsoft products and a greater control over the IT security technology employed by MNCs within their borders, it is doubtful that this deficit will persist for much longer.

3.3.2 **Approaches to Securing Cyberspace for the Nation.** Calls to securitize the nation's vulnerabilities in cyberspace began in the early 1990s, well before recent intrusions in federal systems drove an emphasis on cyber security within the Obama administration. In 1993, while working for RAND, John Arquilla began to popularize the idea of "cyberwar" (Arquilla and Ronfeldt 1993). As he and his fellow author, David Ronfeldt described it, "cyberwar" was an acknowledgement that cyberspace is becoming the critical enabler of modern military command and control. Therefore, a nation or their military's cyber capabilities will become obvious targets in any future conflict. Based on this clear imperative to ensure secured access to cyberspace, several researchers have explored varying strategies to achieve this goal. These strategies extend beyond the basic economic considerations discussed in the first section of this work. They can be divided into military, commercial or economic, technological, and political approaches.

Probably the most comprehensive work regarding the potential for military conflict in cyberspace has been written by Greg Rattray. In his book, entitled *Strategic Warfare in Cyberspace,* Rattray (2001) presents a convincing argument that the effort required to both effectively secure cyberspace against a concerted attack, and to develop the capability to launch an attack achieving militarily effective objectives, demand resources that only an advanced nation-state can muster. His analysis compares the development of a cyber warfare capability to the development of a strategic bombing capability. Based on this case study comparison, the US, for example, would be considered to still in the early stages of building an effective military capability to attack targets in the domain, despite the presumptions in Hollywood and the media. Were this the case, it would suggest that few, if any, technologically advanced nations would be prepared to conduct operations in cyberspace in the same manner, or on the same scale, that they conduct military operations in air, land, or at sea.

Martin Libicki, from RAND, holds a differing view of the effectiveness of using the military to counter threats in the domain. Perhaps in acknowledgement of the tremendous effort it would take to build a robust force, or because he thinks such a force would be so easily countered by inexpensive software measures as to render its development pointless, he recommends the path of assimilation (Libicki 2007). According to his assessment, the United States should leverage its current leadership in setting standards and providing content to generate a cyberspace that is so inextricably linked together internationally, any attack on the US, specifically on the US component of the Internet, would cause the effects to be felt by the attacker as well. In a way, this strategy is reminiscent of the deterrence strategy of mutually assured destruction. Its usefulness, however, is limited to ensuring the functioning of the commercially available Internet. While this is a critical component of the nation's use of cyberspace, such a strategy may be a less-effective deterrent against more precise attacks against such targets as control systems or espionage. Such a strategy would also fail to deter other, non-state or lesser-developed state actors who would still not be connected on a wide-scale and therefore vulnerable to the repercussions in the domain.

The last major "solution space" is championed by several in the computer science community. While recognizing that there are limits to technological solutions, researchers in this camp still focus on technology research, and on maintaining a national lead in technological security measures. The book, *Toward a Safer and More Secure Cyberspace* (2007), by Seymour Goodman and Herb Lin, contains a recent example of this approach.

Goodman, one of the nation's leading cyber security researchers, and his co-author conducted an in-depth assessment of the state of cyber security technology in the United States. According to their findings, the nation's most urgent need is an expansion of cyber security research and education. In their words:

> "…collaborations must be undertaken as enterprises among co-equals—and in particular the computer scientist as cybersecurity researcher cannot view the problem domain as "merely" the applications domain, must refrain from jumping to conclusions about the problem domain, must be willing to learn the facts and contemplate realities and paradigms in the problem domain seriously, and must not work solely on the refined abstract problem that characterizes much of computer science research (Goodman and Lin 2007, 65)."

This statement is a clear acknowledgement that current research lacks a more comprehensive consideration of the cyber security dynamics. Research should consider such factors as the motivation of malicious actors, the fact that security measures are employed by non-technical experts, and that economic factors often over-ride security concerns when firms choose IT tools.

3.4 **Cyber Security and Organizational Behavior**. While the study of organizational behavior is clearly important to understanding national security issues in cyberspace, unlike in the above two fields, a straight-forward "sub-categorization" of relevant research agendas is more difficult. In fact, none of the works presented in this literature review contain organizational behavior research specific to national security in cyberspace.

Therefore, the research presented here focuses on organizational communications, building trust between organizations, and overcoming the principal/agent problem present in large organizations. This section will be organized along a general spectrum moving from government organizations, to the private-public partnership, and finally to private organizational behavior. The first section will contain a discussion of two seminal studies on government bureaucracies and effectiveness. Since national cyber security efforts are managed and coordinated by no less than four major governmental departments, any efforts to improve the nation's security posture must account for the functioning of these large bureaucracies. The second sub-section will move to literature that addresses inter-organizational governance and interactions. Another major component of cyber security is the necessity to foster public-private partnerships. Much of this research focus on the critical role that 'trust' plays in these relationships. The last sub-section focuses on the collective action of organizations. Many of the actions required to improve national security in cyberspace require the collective action of firms, trade associations, and various other organized collections of economic or political actors. In fact, US national cyber security is ultimately dependent on the collective actions of nations and other non-state actors in the international system.

3.4.1 **Government Bureaucracy.** James Wilson (1989), in his book, *Bureaucracy,* has written the most influential work on government bureaucracies.[15] Wilson, in his characterization of bureaucracies, brings up two related factors that aptly describe the federal agency most responsible for national cyber security, the Department of Homeland Security, and its relationship with the external interests in the private sector. First, he describes the political environments in which an agency like DHS would exist calling it "entrepreneurial." He describes such an environment as one where the costs are heavily concentrated on specific industries while the benefits are experienced by a much larger population, in this case, the US public (Wilson 1991). According to Wilson, one of the biggest challenges confronting an agency in this situation is that it has a discreet collection of organizations hostile to its activities, but no organized support base when things are going well. In the case of DHS, when their job is done well and there are no homeland security issues, Congress and the general public give them little support.

Wilson also categorizes federal bureaucracies by the nature of the operations they conduct. He divides them up into production, procedural, craft, or coping organizations (Wilson 1991). Again, DHS easily falls into one

[15] This book need not be critiqued in any way other than to comment that it is painfully accurate in its assessment of the Office of the Secretary of Defense, in which this researcher is currently employed.

category, the coping organization. According to Wilson, these organizations can "observe neither the outputs or outcomes of their key operators." Except for managers at the security checkpoints in airports, most supervisors cannot closely monitor the actions of their operators nor can they accurately assess the effectiveness of their actions. As long as something does not go wrong, it must be assumed that the operator is effective. In the case that something does go wrong, it may not be attributable to poor work, but DHS will assuredly receive the blame. In cyber security matters, for example, any positive impacts of DHS's efforts will go largely unnoticed and be almost impossible to measure. One can imagine that this dynamic causes a host of managerial problems in a coping organization and can lead to significant morale issues. Perhaps this structural issue helps explain why the DHS Computer Emergency Response Team has had five directors in the last six (Nakashima 2009).

Graham Allison (1969) conducted an even more critical analysis of the workings of government agencies in his analysis of the Cuban Missile Crisis. While Wilson provided insight into the motivations and dynamics that drive bureaucracies in order to show how their action is ultimately rational, Allison provides a compelling argument that it is quite possible there is no logical explanation for the ultimate 'output' of the agencies involved in formulating and executing security policy for the nation (Allison 1969). Allison demonstrates this by presenting two alternatives to the rational policy model, the third being a model of bureaucratic politics characterized by bargaining games. In the words of Allison:

> Men share power. Men differ concerning what must be done. The differences matter…More often, however, different groups pulling in different directions yield a resultant distinct from what anyone intended. What moves the chess pieces is not simply the reasons which support a course of action, nor the routines of organizations which enact an alternative, but the power and skill of the proponents and opponents of the action in question (Allison 1969, 707)."

Perhaps in an organization such as the Internal Revenue Service, the bureaucracy may "run the show." But in agencies such as DHS and DOD, the Secretary and senior leaders ultimately have the final say on the direction the agency and the nation will take. Any political bargaining they conduct will be done in the context of all the other issues of significance to their agency. Not only will these leaders have differing opinions on the issue at hand, but also on the myriad of other issues that influence and are influenced by the outcomes of a particular issue, such as national cyber security. There is little empirical data regarding the impacts of poor security in cyberspace, or the immediacy of threats, to support rational policy making. Therefore, the bureaucratic policy model provides a compelling alternate perspective on how, or if any, policy measures are enacted to enhance cyber security.

3.4.2 **Inter-Organizational Interaction and Governance**. An oft-repeated phrase in discussions regarding critical infrastructure protection is the “imperative of public-private partnerships.” But how are these partnerships defined and how are the fostered? In most cases, the partnerships under consideration are between federal government agencies and private organizations and firms. The development of these partnerships is a major theme of *Seeds of Disaster, Roots of Response*. In the contribution by Lewis Branscomb and Erwann Michel-Kerjan (2006), they note that challenges to building these partnerships, from a regional to international level, come from different habits and cultures, and the “legal, political, and financial power among a complex mosaic of stakeholders (pg 395).” In their view, the essential element of successful partnerships that will endure at an organizational level is the creation and maintenance of trust between actors in the partner organizations. Ultimately, this trust must be institutionalized such that it survives the turn-over of personnel in relevant organizations. In other words, the trusting relationships must become part of the culture of the organizations. Such acculturation is a long-term affair. Todd La Porte and Daniel Metlay (1996a) created a term for this called, “institutional trustworthiness.” According to La Porte and Metlay, when an organization has lost its status as being trustworthy, it means that “many of the members of the public and stakeholder groups believe that the organization neither intends to take their interests into account nor would it have the competence/capability to act effectively even if it tried to do so (pg 342).” One could imagine how demoralizing it could be to work in an organization for which the public has such a perception. However, La Porte and Metlay provide several suggestions on how an organization can regain or maintain its institutional trustworthiness. Not only do they focus on such straight-forward issues such improving engagements with outsiders, but they also recommend qualitative changes to those engagements such as involving more senior personnel and more integration with affected communities (La Porte and Metlay 1996). In addition, La Porte and Metlay suggest that improvements to internal operations are critical because improved internal processes also generate an additional source of reassurance. Such measures point to changing the impression that the organization "couldn't get better even if it tried." In coping organizations like DHS, this imperative is especially clear. The constant rotation of US CERT Directors is not only detrimental to effective, day-to-day operations, it is also detrimental to efforts to establish long term trust with outside organizations.

One of the best, and often quickly executable, steps to developing a more trusting relationship is to improve information-sharing. This is the topic of Daniel Prieto's (2006) contribution to *Seeds of Disaster, Roots of Response*. Prieto highlights significant impediments to the exchange of information both to, and from, the private sector. For example, private firms consider information regarding the cyber security of their operations to be an asset that, once disclosed, may put them at a disadvantage to their competitors. As identified earlier, disclosure of cyber security vulnerabilities may also create a liability for firms when working with customers or law enforcement. On the other hand, federal agencies may confront barriers to sharing information with private firms because of the classification of the information, specifically regarding foreign nation-state threats, or because disclosure may impede an on-going law enforcement investigation. Prieto accurately portrays the dilemma created by this stand-off. Though public agencies are simply frustrated by the reluctance of private firms, private firms, on the other hand, think that the government is unnecessarily withholding valuable information (Prieto 2006). According to Prieto, it is more likely the case is that these agencies have little valuable information to provide to private firms and have trouble managing, collating, and transmitting information of value that they do have.

As the reviews to this point have demonstrated, there are many institutional barriers to turning bits of data into valuable knowledge. The answer is not necessarily in creating better Information Technology (IT) networks. In many ways, federal agencies like DHS, and DOD, must realize that, for them to integrate effectively with private firms providing for national security in cyberspace, they must view themselves as organizations that provide the product of knowledge. According to Thomas H. Davenport and Lawrence Prusak (2000), in their article, "Working Knowledge: How Organizations Manage What They Know," enormous expenditures on technology initiatives have rarely delivered what the organization needed or thought they were getting. What organizations must do is make the leap from data collection, to adding value to data to generate information, but then also to effectively managing knowledge. To Davenport and Prusak, knowledge is a "fluid mix of framed experience, values, contextual information, and expert insight that provides a framework for evaluating and incorporating new experiences and information (pg 5)." While IT systems may provide the network that will allow the exchange of knowledge, federal agencies must work hard to improve their knowledge level in order to share information, and, ultimately, value-added knowledge, if they expect other agencies and private organizations to reciprocate.

Another way to improve information-sharing and trust is to establish inter-organizational social, not necessarily formal, networks. However, the creation of informal networks also comes with its own challenges. As a group of Australian public sector governance researchers have identified, the solution to many highly complex and intractable social problems requires the establishment of inter-agency network structures (Keast et al. 2004). Keast et al., state that network structures, as opposed to personal, informal networks, arise between organizations and result in entities such as task forces to accomplish broad missions and “strategically interdependent actions.” They caution that there is a high degree of risk involved in that the commitment that members have to the goals of their own organizations does not disappear and that trust is not easy to build. Most significantly, they suggest that the results achieved through network structures do not have to do with generating easily quantifiable programs or products, but “have more to do with changing relationships and perceptions (Keast et al. 2004).” Regardless, the US federal government needs to appreciate the benefits of such improvements to processes even if they are not directly quantifiable by participating agencies. David Thacher (2004), in a case study of a New York community security initiative seems to confirm the conclusion from the Australian research team. He adds that when a partnership works well, it creates a conflict of interests for the personnel assigned to the team since, as noted by Allison, all agencies have their own perspective on the problem (Thacher 2004). According to Thacher, “it saddles them with new responsibilities and even a new outlook to integrate them into a work group and its mission (pg 102).” The irony is that the more effective the inter-agency task force becomes, the more the members become viewed as “traitors” to their own organizations. Inevitably, the member may have to choose between home agency or the new partnership. Thacher’s main conclusion is that the partnership that survives, overcomes challenges to coordinated action, and grows, will ultimately form the basic structure of a new hierarchical organization. This conclusion suggests that there is the possibility to codify a “joint team” within the agencies that contribute to national cyber security. With the Goldwater-Nichols Act of 1986, Congress mandated a joint team within the US Department of Defense. Perhaps a similar construct across the US federal government can evolve if enough emphasis is placed on a joint partnership between DOD, DHS, and DOJ.

But even if this joint team improves the federal agency coordination, it does not solve a basic problem highlighted by Myriam Dunn-Cavelty and Manuel Suter (2009) regarding expertise in the area of cyber security. In their article calling for a new governance model for critical infrastructure protection, these authors suggest that advanced nations, because of the technological complexity of their infrastructure, should rely on self-regulating networks. Since the federal regulators cannot be expected to have the expertise required to understand the unique cyber security issues of every control system and IT system in use, effort would be better devoted to fostering and over-seeing self-regulating entities (Dunn-Cavelty and Suter 2009). Dunn-Cavelty and Suter support the idea that building mutual trust will be more effective than attempts at government control. Unfortunately, the difficulty in measuring trust levels compared to control levels will make such an approach difficult to sell to legislators.

Zaheer and Venkatraman (1995) have conducted one of the few empirical studies to show the benefits of creating trust-based networks that ultimately become formal relationships between firms. Of significance, they demonstrated that trust is a positively and significantly reinforced by close integration, but also that this feedback benefit of a trusting relationship may lead to a situation where a relational contract is costlier to terminate than a discrete contract (Zaheer and Venkatraman 1995). Their results conceptually apply to relationships between private and public organizations equally well. This finding would suggest that, once DHS has begun to develop a strong information-sharing network with private organizations, the firm may eventually formalize the relationship as an inter-organizational strategy. The termination of this relationship could become costly to the firm even if the information-sharing relationship never becomes a regulated activity (a discrete contract).

Another way to conceptualize the value created through a strong-information-sharing network is through the concept of "social capital," or a creation of capital that forms from relations between and among actors and the obligations they create with each other. According to James Coleman (1988), who defined this concept, social capital consists of the creation of "relations among corporate actors that can constitute social capital for them as well (pg 98)." Though less tangible than physical capital, there is no doubt that, as a component of human capital, “social capital” improves productivity of an organization. In short, there are potentially significant economic advantages to building relationships between public and private actors. Through their bi-annual response exercise, Cyber Storm, DHS has made an effort to build its social capital through the simple act of holding several planning events for the exercise at which federal officials and representatives have the opportunity to meet and trade business cards (DHS 2010a).

3.4.3 **The Economics of Collective Action.** At this point, it is useful to return to an economic perspective of inter-organizational cooperation. The cooperative entity of interest is not one related to cartels, such as collusion for the purpose of price-fixing, but a cooperative for the provision of a collective good. The issue of collective or public goods, negative externalities, and cyber security was raised in the economics of cyber security field. However, the dynamics of the organizations within the collective was not the focus of the analysis. The works in this section analyze the direct and indirect influence the actors in the collective have on each other. This is an important consideration because, at the level of the industry, the positive or negative cyber security externality is created by a collection of firms, an interdependent sector. Their behavioral motivations must consider that the actions of any one firm in the sector will influence the actions of others. Also, as relates to the information-sharing network discussed above, the product of that network can be classified as a public good. First of all, the network theoretically creates a good of value in the form of important information regarding cyber threats and effective defense techniques. Secondly, the good is non-rivalrous because sharing the information with any one firm does not reduce the value of the information to any others in the network. Third, even though DHS could exclude a firm from the information-sharing network, it will not do so to avoid being liable for neglecting the public good of national security thereby making the good non-excludable.

Clearly, the seminal work on collective action and its motivations was conducted by Mancur Olson. In, *The Logic of Collective Action*, Olson (1971a) contests the common perception that large collective groups, for example unions or trade organizations, can exist through voluntary contributions to further the common interest of the groups. The problem is, without some form of compulsion, the members who can reap the benefits of the group's action without paying any dues will quickly cease to contribute and free-ride on the backs of those who receive a marginal individual benefit from the good that is greater than the cost resulting from their participation. In other words, in the case of major contributors, a decision not to contribute will be immediately felt by the contributor and it will cost them more than if they contributed. However, for those smaller actors who will not reduce the overall provision of the good when they shirk, the incentive to free-ride is overwhelming. According to Olson, in a small group, there may be an incentive for a potential free-rider to contribute because the actions can be monitored and anyone's non-contribution will be likely to be felt by all. But as the group gets much larger, the small players will have no incentive to pay their dues to be in the collective if there is no way to make any provision of the good individually selective to everyone's contribution.[16] Olson also demonstrates mathematically that even in small groups, there will be a tendency to under-produce the collective good and the under-production will increase with group size. This observation is consistent with the observations of authors presented earlier in the discussion on reducing negative externalities and providing a collective good of cyber security.

As stated earlier, the information-sharing network can also take a straight-forward form of a collective good. However, a critical, yet undefined, number of actors must contribute to creation of this good. If an insufficient number of members are in the group, there is not enough of a contribution to

[16] Of note, he suggests that one form of selective benefit in a collective is the "social incentive" (Olson 1971a). According to Olson, "social status and social acceptance are individual, non-collective goods." This is an interesting semantic point. In my opinion, it becomes difficult to draw the line between the collective good and social acceptance. For example, if one thinks that doing good for others, the collective good, is something that makes them feel better, then what is the difference between saying the actor contributes for common interest or self-interest? Therefore, I think it can be argued that Olson built up a straw man when he disputed the writings of sociologists about large groups. In fact, most probably, his theory applies to special cases, such as unions and other economic groups, vice collective action in general. It seems it would not to apply to a large number of groups in existence, for example, environmental organizations and philanthropic societies, which are probably the type of organizations being referred to by most of the authors of which he was critical.

produce a good that is value-added. As when a small community cannot collect enough funds to build a pool, there is not enough information being provided to the DHS cyber security centers for them to collate, fuse, and re-distribute a valuable product. If this were the case of a club good, defined by James Buchanan (1965) to be mostly non-rivalrous but excludable (e.g. a community pool), as long as enough members are induced to contribute to a "value-possible" level, there would be a potential to generate a sustaining information-sharing network. This outcome would be possible because, once firms start receiving a value-added product, they will continue to contribute to avoid being taken off the distribution list for the information product. Public action would only be necessary to "prime the pump" to get to a value-added level of information-sharing and then the threat of exclusion would maintain the contributions. However, from the public sector perspective, this information-sharing network is arguably *not* a club. The government cannot purposefully cut non-contributors off from any data DHS could provide to critical infrastructure operators because denying important information to a non-contributor in such a sector would be willfully neglecting DHS's responsibility to protect the homeland.[17]

[17] Of course, the firms know this, so each of them sits and waits for information from DHS and other governmental agencies, but contributes little if anything, thereby ensuring that no one will get anything useful and DHS will appear ineffective as a coordinator and clearing house of cyber security information.

Perhaps, one form of motivation that DHS can appeal to is the "social incentive" that was theorized by Mancur Olson as discussed above. It may even be possible for DHS to leverage the "social incentive" aspect of trade associations and sector-internal private legal systems (PLS) to promote improved cyber security. In a recent contribution on forming legal cyber security enforcement mechanisms, Amitai Aviram (2005) assesses the potential for organizations, such as sector information sharing and analysis centers (ISAC), to achieve this task. He does so with the goal of determining where public subsidies, such as the provision of threat information to the CI firms, will be most effective. According to Aviram, a new collective action norm is more likely to be enforceable when the existing PLS can threaten the members with exclusion from a previously available benefit. Otherwise, using ineffective PLSs, or attempting to generate new ones, will result in a waste of any attempted public sector support because compliance with the desired measures cannot be secured (Aviram 2005). Aviram's theory is an important consideration when comparing the effectiveness of sector ISACs. In sectors where the ISAC has been shown to be a beneficial entity for improving cyber security, this observation is may be due to pre-existing, strong relationships in the sector. Avrim gives the example of the chemical sector as one in which existing interaction is effective. In others, greater direct involvement in cyber security by the public sector may be a necessity because private networks cannot be expected to form spontaneously and succeed in improving cyber security.

To conclude this section, I will return to a special example of collective action considered by both Mancur Olson and Thomas Schelling, that of the defense alliance. In an empirical analysis that Mancur Olson conducted with Richard Zeckhauser (1966) on the North Atlantic Treaty Organization, the authors sought to demonstrate that Olson's theory regarding the under-provision of collective goods by their collective can also apply to this unique form of collective. In this work, the authors showed empirically why, even though all members agreed that a certain level of military capability was required in the face of the very real threat of the Soviet Union, they never reached that level of capability as a group. Just as in the case of organizations formed for common economic interests, the smaller organizations took advantage of the security umbrella provided by the larger members (Olson and Zeckhauser 1966). This is an important conclusion since it demonstrates that, even in situations where participants are contributing to a clearly important public good, the common defense, there will still be a tendency to under-provide the good from a common perspective. The authors did note a paradoxical conclusion from their analysis in that, should the unity of the alliance decline, and the members expect that their expense on defense be more privately appropriable, they may have a greater incentive contribute more (Olson and Zeckhauser 1966, pg 272). In this case, so long as the alliance holds when needed, it may function better in a tenuous agreement than when it demonstrates more unity. This conclusion is logical if a country determines that their ability to defend themselves is not always dependent on the ability of others in the alliance. In other words, they are not completely dependent on the weakest link. However, this condition does not hold for all alliances. For example, in the case of inter-networked computer systems who are defending against espionage intrusions. If any one computer in the system is penetrated, “the borders” between them and the other computers may also be penetrated without a defense. Once the intruder is in the system, they may not be challenged again as they traverse corporate LANs. This type of situation creates the opposite effect of what Olson and Zeckhauser noted regarding disunity. As will be demonstrated in Part III, a perception that others are not contributing to the common defense in such a system will cause a severe *dis*incentive to invest.

Although Thomas Schelling wrote extensively about strategy, security, and conflict, his work that is most applicable to national cyber security is an article in which he did not discuss defense issues specifically. In Schelling’s (1973) article regarding binary choices, the Nobel laureate described the concept of binary, “either-or,” choices that create externalities on the decisions of others. To explain the concept, he described several different situations, from restrictions on whaling, to the wear of hockey helmets, where the question was not about how much anyone does, but how many make one or the other choice. The interesting implications of Schelling's model was the potential for a "minimum coalition" to overcome a stable decision equilibrium where everyone was previously worse off, and the potential to "tip' the entire collection of decision makers from one decision to the other. This tipping effect could reduce the potential social costs (increase the public benefit) when not enough actors make the socially beneficial choice in the absence of any incentive to do so. This is a potentially significant consideration in the area of cyber security. For example, consider the case when a firm recognizes there is a need for implementing cyber security, but there is also a significant cost. If the success of the security measures is significantly dependent on a similar investment decision by others in an interdependent system, there is an extreme disincentive to incur the cost of investing, even though everyone knows that the entire system would be better off if everyone were investing. The problem is one of coordinating the right binary decision. Though Schelling described a general case of this model in his paper, he did not anticipate the endogenous effect of a growing coalition and the probability of attack against those who remain out of the coalition. In fact, if a large group of firms were induced to invest, a point would be reached where the cost for those who chose not to invest would become marginally greater as the cyber attackers chose to chase the “weaker members of the herd.” This effect would theoretically hasten the move toward a system where all are fully investing in security. Though a negative externality would be reduced, such actors are not motivated to produce a common good. They would clearly be making an investment decision to achieve the private good of security for their firm. The fact that they are in the “defense alliance of cyber security investors” is not as much a conscious decision to join a group to create a collective good but better described as a categorization based on their binary decision.

3.5 **Summary**. In this part, I introduced the research agenda for this dissertation and made the argument for considering aspects of cyber security to be components of national security. Although most the literature review and analysis in this dissertation relates to the United States, the propositions contained herein are intended to be global. Ultimately, nation-states have two options to reduce their insecurity; they can either make themselves less vulnerable to security threats, or attempt to prevent or lessen perceived and real threats (Sundelius 1983). The literature review above provided an overview of the academic research focusing on ways to make a nation less vulnerable to security threats and some ideas for influencing the threats. Strong arguments can be made for taking either, or both routes. Even if all stakeholders agree that a threat should be securitized, it does not guarantee agreement on the correct response to the threat. Wolfers (1952) provided a useful illustration. If one nation had a policy to maximize its security by relying on armaments and alliances, while another did so based on maintaining strict neutrality, “a policy maker would be at a loss where to turn (Wolfers 1952, 490).” In cyberspace, there are many proposed solutions to addressing a wide array of threats. Some stakeholders advocate for stronger regulations while others question the effectiveness of existing government oversight. As long as there is private ownership of the nation’s critical infrastructure, this debate will continue.

Part I of this dissertation has made the argument that the private sector must play a leading role in contributing to the nation’s security in this area. Two specific actions that must be undertaken at a level beyond the business case are substantial investments in cyber security measures and the contribution of information to the national preparation and response networks. The next two parts contain research analysis and discussions that will address each of these two actions.

Part II

Cyber Security Investment Decision in an Interdependent System[18]

[18] Significant portions of Part II have been adapted with permission from a forthcoming article to be published in the International Journal of Critical Infrastructure Protection. The article was co-authored with Jon Goldstein, also of George Mason University. Jon Goldstein conducted the coding for the agent-based model and provided helpful feedback on its functioning. However, all pseudo-coding (instructions for the way the model should behave), analysis, and interpretation of results used in this dissertation are solely those of the author.

4 Introduction and Prior Work

4.1. **<u>Overview</u>.** As stated in Part I, this research seeks to examine the challenges the federal government faces in fostering private sector contributions to the nation's cyber security. Among other things, the nation's security in cyberspace is improved by reducing and ultimately removing potential security externalities created by insufficient security investments and ineffective levels of information-sharing. In Part II, I will explore the issue of insufficient investments in cyber security measures. As discussed in the literature review, the investment decision is complicated by a host of unknowns. Many of these unknowns, such as the understanding of the return on investment lead directly to the insufficient levels of investment. In the face of these unknowns, researchers have introduced models that have been simplified to some extent to try to further our understanding of investment decision-making. For the purpose of this research, the cyber security investment decision is modeled as a binary choice that depends on the actions of others.

In his 1978 book, *Micromotives and Macrobehavior,* Nobel laureate Thomas Schelling (1978) investigated the dynamics of such binary (i.e., either-or) choices that have an impact on, or create externalities for, the decisions of others. To explain the concept, he described several different situations in which a person's decision depends not on how much any individual does but on how many people make one choice or the other. For example, the decision to follow daylight savings time or join a boycott would be a binary decision that creates an externality for the decisions of others (Schelling 1978); that is, a person is presumably more likely to join a boycott when many others also participate. One interesting implication of Schelling's model is its potential to "tip" a collection of decision-makers from one decision to the other. Inducing such a tip could reduce the potential social costs if, before the tip, too few actors make the socially beneficial choice or, conversely, increase the benefit at an increasing rate when more actors make the right choice.

The model could also be applied in situations where actors must coordinate security decisions such as the investment in cyber security measures. As discussed in the literature review, economists Kunreuther and Heal (2003) built on this concept of interdependent decision-making after the events of 9/11. They introduced a game-theoretic approach to explore more deterministic outcomes of a class of binary choices, the interdependent security investment (IDSI) decision. Their focus has been on the IDSI problem and the existence of Nash equilibria in games where players decide whether or not to invest in security measures. An important yet counter-intuitive aspect of their model is that actors will be inclined *not* to invest in security when a particular risk of attack increases. This is the risk of attack that is created when others in the interdependent system are not investing (Kunreuther and Heal 2003). Though it is an externally-generated risk against which the actor cannot defend, I will call this the "system-internal" threat of attack because it emanates from within the interdependent system of actors. Extending the Kunreuther and Heal model, Zhuang and Bier (2006) argue that even a single attack directed against an interdependent actor attack, or one emanating from another actor within the system, could be catastrophic because it might result in "death, loss of reputation, or theft of a valuable trade secret."

According to cyber security author Ira Winkler, a single attack of information theft in the defense industrial base could be disastrous. In a recent interview, Winkler stated that due to military technology's importance to national security, one weak spot could be "catastrophic" (O'Hara 2008). As identified in the introduction to this dissertation, recent incidents have reinforced Winkler's concern. The most sensitive computer systems in the defense industrial base, those that design the flight controls and defenses, are not publicly accessible on the Internet. However, many other interlinked systems, which the contractor organizations are responsible for securing, are accessible. If a substantial amount of data can be obtained from these marginally secured systems, such as those that are responsible for diagnosing the maintenance problems in the joint strike fighter, would-be international competitors can still gain a significant advantage (Gorman, Cole, and Dreazen 2009). Importantly, all major weapons systems are developed by teams of private industry, prime and subprime contractors that must share, and protect, this sensitive technological data. While no lives may be lost as a *direct* result of the theft of this data, disclosure of the details and potential vulnerabilities of major weapon systems could lead to a comparable catastrophic loss in a future conflict. More directly, inadequate security measures that are penetrated by cyber spies could lead to substantial penalties for the firm responsible for the loss, or a loss of trust from its customer base leading to cancellation of future contracts. Therefore, cyber espionage in this critical sector of the nation's infrastructure should be analyzed as an interdependent security problem.

In this part, I will apply the IDSI model to the cyber security investment decision using a sample network of the defense industrial base. The focus of this analysis is an extension of the IDSI model that will consider the underlying network that characterizes interaction, based on program partnerships, within this sector. The information-sharing network is based on actual contractual relationships comprised of a sample of firms from defense industry trade associations. I introduce this contract-based social network topology to examine the impact of the network structure on tipping and cascading in the security investment decisions made by actors within the sample.[19] I use the agent-based modeling technique to explore how interaction within a certain network topology may influence the agents' ability to gather investment information, and thus influence policy-maker measures to induce tipping and cascading investment in cyber security.[20] The agent-based model allows me to relax some of the strict assumptions of the underlying game-theory approach and to observe dynamic decision-making behavior. I find that changing an actors perception of pooled risk, as assumed in the IDSI model, may lead to substantially different investment behavior; for example, agents acting within a scale-free interaction network may decide to invest in security measures when faced with much higher risks from indirect attack than if they had perfect information on the investment decision of all other agents in the system. Conversely, the network structure

[19] By "topology" I mean the network structure in which the actors are functionally arranged. Some common topologies are lattices, random graphs, small-world networks, and scale-free networks. It is also important to note that this network is not a logical connection of computers per se. It is only a model of interaction.

[20] Schelling's concept of "tipping" was introduced on page 1 of Part I. Heal and Kunreuther (2007) explain "cascading" as "inducing some agents to invest in protection will lead others to follow suit." Cascading may occur without the system tipping to a state of most or full investment.

may contribute to resistance to tipping toward an equilibrium at which all actors have chosen to invest. In other words, the onset of investing behavior may occur at a much higher level of risk from system-internal attacks, but cascading or tipping to a 100 percent investing equilibrium occurs over a much greater range of externally generated risk. Importantly, I find that the model continues to function in a stable manner when changing risk perceptions and limited, non-rational behavior, are also introduced to the model. All these factors may influence the creation of an investment coalition intended to tip the system to a state of sufficient investment against concerted cyber threats. In the next section, I present a brief summary of prior work related to this research methodology. The focus will be on methodologies used for this analysis since these works were not presented in the literature review in Chapter 3. The methodology chapter describes the generation of the sample network and explains the agent-based model developed for this analysis. In Chapter 6, I identify key findings based on several iterations of the model. Conclusions and public policy implications are left to Part IV.

4.2. **Prior Work.** The analysis in Part II builds on research in several diverse fields, such as the economics of information security, game theory, and social network analysis. In the most general sense, the problem of cyber security investment is a case of binary decision-making that depends on the number of others confronted with the same choices who decide on a particular one. A game-theoretic approach can predict decision equilibria in actor decisions that are based on the expected payoffs while also considering the decisions being made by other actors. Schelling (1978) provided a collection of relevant examples of such decisions, from whale hunting to concealed gun laws. In their 2003 paper, Kunreuther and Heal (2003) formalized the interdependent decision-making analysis in a game-theoretic model, which provided mathematically deterministic equilibria based on the initial values of a set of specific parameters. They also demonstrated mathematically how the collection of actors could be tipped from an equilibrium of non-investing, or a mixed equilibrium, to one where the entire system chooses to invest in security measures. As discussed previously, several authors have applied Kunreuther and Heal's model to different scenarios. In addition, researchers have extended the basic game-theory approach to account for actors discounting risks and possibly making erroneous choices (Bier and A. Gupta 2005). In many cases, researchers considered the impact of relaxing strict assumptions; each attempt to do so makes it increasingly difficult to calculate equilibria in the basic game-theory framework. Therefore, introducing an agent-based model allows one to analyze the decision-making process in a more dynamic manner.

One important consideration for decision-making is the interaction space of the relevant agents. As Kunreuther and Heal (2003) theorize, it is possible that all actors in a system may be impacted by the security decisions made by all the other actors. This situation could be considered one of "pooled risk" for the whole system. In a network sense, the network would be considered completely connected.[21] For agents to effectively incorporate others' investment decisions in their own, they would be expected to have "perfect vision" into the actions of the complete network. However, researchers such as Watts (1999) and Granovetter (1973) have demonstrated that the actors' communicating, negotiating, and decision-making can be influenced significantly by the structure of the social networks existing between the actors, regardless of the actual risk imposed by the actions of others. According to these researchers, the characteristics of the network, such as clustering and path lengths between actors, should influence the network's tendency to exhibit tipping or cascading (Watts 1999). In effect, social network analysis has made an important contribution by realistically constraining the interaction space of the decision-makers. Network theorists have also found that specific networks, such as those that exhibit small-world

[21] This case, which is limiting from a network standpoint, is the common assumption for most economic models of interdependence. For example, "externalities" are most often assumed to be experienced by all actors in an economic market.

or scale-free characteristics, tend to strengthen interactions between otherwise loosely connected actors (Wasserman and Faust 1994).[22]

In their work on collective dynamics, Lopez-Pintado and Watts (2008) merge binary decisions and network characteristics in order to classify research models according to their ability to inform policy. These authors have classified the basic IDSI model as mechanistic and note that solving the equilibrium for a specific case, such as airline security, may not provide much utility for other binary decision situations in which the parameters and agent interactions are vastly different. Advances in agent-based modeling concepts allow me to expand the analysis of interdependent decision-making with the introduction of dynamic agent behavior and the interactions of actors with heterogeneous characteristics. According to Axtell (2000), agent-based models are particularly useful when a mathematical model can be derived, but not completely solved, in a complex interaction space.

This introduction and review of related work briefly covered a wide range of research to show how this particular application of the IDSI model can link diverse fields in solving critical infrastructure problems.[23] The next

[22] *Scale-Free Networks*, by Barabasi (2003), provides an excellent explanation of the characteristics of this network type.

[23] In this introduction, I have not addressed the role of the Department of Defense as the sector-specific agency for the defense industrial base. I will briefly mention the DOD in the Discussion section of Chapter 6 and I will also consider their role in coordinating security investment in Chapter 11.

chapter explains the methodology employed to analyze cyber security investment behavior.

5 Methodology

5.1. **Research Question and Hypotheses.** The purpose of Chapter 5 is to present the primary research question and hypotheses for Part II then discuss the methodology employed to explore the stated hypotheses. In Chapters 1 and 2, I identified the critical components of private sector contributions to national cyber security. Private sector actors must increase their investments in cyber security measures and contribute to information-sharing networks that improve security postures and respond quickly to security incidents. In Part II, I will present results of research designed to study ways to coordinate security investment in the face of substantial disincentives to invest.

Research Question 1:

In the absence of directive regulation, how can private firms be motivated to invest in cyber security measures to a level that effectively contributes to national security?

The basis for this research question comes from an assertion in the National Infrastructure Protection Plan (2006):

> "Sometimes cyber assets, systems, networks or other cyber functions may be deemed nationally critical and necessitate additional risk

> management beyond that which the private sector implements as part of their corporate responsibility (pg 121)."

The cyber systems that are deemed nationally critical can be identified at a macro, sectoral level. However, the idea of investing "beyond" the business case becomes more challenging to measure and evaluate. How much investment is sufficient? Ultimately, only an insufficient level can be identified and that is only possible after the national security is threatened. Regardless, it is clear that the current, business case level is insufficient from the perspective of the public good of national security. A much greater level of investment is required on a broad-scale to account for the inter-connectedness in several critical infrastructure sectors and the resulting potential for negative, security externalities. As stated earlier, researchers have developed tools, including the IDSI model developed by Heal and Kunreuther (2003), to aid public policy makers with understanding and implementing measures to foster a greater collective action. Their model provides mathematically deterministic equilibria based on the initial endowment of parameters related to the cost of investment, the cost of a loss, and the probabilities of both a direct attack, or one from within the system. In addition, they demonstrated mathematically how the collection of actors could be tipped from an equilibrium of non-investing, or a mixed equilibrium, to one where the entire system chooses to invest in security measures. The tipping phenomenon was generated by introduction of a minimum critical coalition. According to these researchers, a minimum critical coalition is one "where a change from not investing to investing by its members will induce all nonmembers to follow suit (Heal and Kunreuther 2003, 12)." Unfortunately, the basic model must make certain assumptions that are particularly problematic when applied to a cyber security problem. First, the model requires that the actions of each actor are visible to the others. In the area of cyber security, the only way to be able to assess the implementation of other's measures is to be invited into their network security center and monitor activities there. Second, the basic model requires that the actions of all other actors in the system be considered. In other words, the actors consider their risk to be pooled. However, in the area of cyber security, it may be that certain paths between actors are more critical than others. For example, if a blackout in the eastern electrical sector must flow through a central sector before impacting the west coast, operators on the west coast are more concerned about security measures in place in the central sector than in the east coast. Or it may be that decision-makers will discount the impact to their security from others with which they seldom interact. Third, the risk of both an indirect, system-internal attack and a direct attack (i.e., one that comes at the victim from outside the network to their "front door") are exogenous in the basic model. However, it should be expected that well-protected targets would not be assaulted as frequently as those with less defenses. Eventually, the probability of a successful attack should rise for those who choose not to invest. Lastly, the national security component of a loss generated by a successful attack is much more difficult to measure than the direct economic loss. This challenge makes it extremely difficult for investors to internalize this loss component in their investment decision even if they were prone to do so.

While the tipping characteristics of the model are of the most interest to policy makers the last concern above, the first three concerns must be addressed in order for the IDSI model to be more effectively applied to the national cyber security problem. Therefore, the first hypothesis attempts to address these three points.

Hypothesis 1A: The significant features of the IDSI model hold when introducing into the model the network aspects of interaction between firms, an endogenous risk of direct attack, and the potential for non-rational decision-making behavior.

Hypothesis 1A both relaxes assumptions inherent in the basic IDSI model and allows for a more empirically rigorous interaction landscape. First, it relaxes the assumption of perfect information regarding all others' investment decisions. As stated above, such an assumption is probably unrealistic considering that the security investment decisions of all other firms, an important component of the cost-benefit analysis, will not be visible to each firm. By introducing the interaction space derived from a program-partnership network, the actors can conduct their investment decision calculations based on a more realistically bounded amount of information regarding others' behavior. This hypothesis also incorporates the endogenous nature of risk. In reality, an attacker will most likely probe for weak defenses and focus attacks at the weakest link. Those who do not invest could be expected to face a higher risk of attack. This increasing direct risk should increase their incentive to invest in security measures at the next opportunity. Finally, this hypothesis incorporates the fact that firms may not act in a way that is considered rational based on this investment calculation alone. Firms must consider a host of opportunity costs of the investment that will also be different for each firm. There is also the possibility that structural forces related to other dynamics within their firm may influence investment decisions more than this specific, quantitative analysis would.

According to this hypothesis, relaxing these assumptions within an agent-based model will not adversely impact the ability of the model to predict such features as mixed equilibria, cascading, and tipping toward a state of full investment. To the contrary, some of these should strengthen the model's predictive power.

With a successful test of Hypothesis 1, the study then focuses on the potential of an initial coalition of actors who invest in security—the primary concern for the public policy analyst.

<u>Hypothesis 1B:</u> In an IDSI model as modified above, coordinated action of a small coalition of firms in a CI sector can tip a sector toward full investment. This action is effective in the face of a significant threat of security breaches emanating from with the sector.

For the purpose of this research, coordinated action entails any action that facilitates the decision to invest by the members comprising an initial coalition. This initial coalition would ostensibly be a collection of actors significantly smaller than the entire population so as to allow for minimal efforts at coordination. The specific number of firms in the initial coalition that would comprise a critical coalition is indeterminate a priori and is most certainly different for each sector of critical infrastructure confronted by an IDSI problem. In fact, as this research will demonstrate, the make up of the coalition cannot be determined until the population has been tipped to a state of full investment (a distinct drawback of static game theory). "Full investment" implies the investment is occurring at each firm to the level sufficient to contribute effectively to the public good of national security in cyberspace. Again, the exact level of investment required cannot be explicitly determined for each firm in the absence of information on attacks that have been successfully thwarted. The assumption is that the appropriate level will be much greater than current levels. Full investment also implies a situation in which all firms are induced to maintain this level of investment. Ideally, the most efficient result would be for this state to be maintained in the absence of regulation that comes with enforcement costs. Lastly, the hypothesis requires this initial coalition to be a critical coalition when the probability of system-internal attack, or an attack that occurs through another actor in the system, is at a realistic level (for example, greater than 20 percent). In the basic model, previous researchers have demonstrated that this occurrence is mathematically probable. In other words, Schelling has determined theoretically, and Heal and Kunreuther have demonstrated mathematically, that a critical coalition can tip a population from one state to another when their coordinated action would make the second state advantageous. This research takes us past these theoretical predictions by both relaxing the strict assumptions in the basic model and employing empirically-derived data to more accurately model the interaction and decision space of the firms.

As suggested by Coase (1960), it is important to apply a theoretical model to an empirical situation before suggesting changes to the model or introducing policies. Constructing a generic, agent-based simulation of the IDSI model does not in itself achieve this imperative because the agents may not be interacting in a manner observed in reality. Without first considering realistic parameters, agents' decisions will not necessarily be based on practical calculations. Therefore, the present research utilizes an empirically based framework created from an inter-firm, contract-relationship network, within which agents in our model interact. Furthermore, attempts were made to endow the actors with decision-making parameters set within realistic bounds, specifically those related to costs of cyber security measures. The next two sections describe the compilation of the network sample and then explain the components of the agent-based model that were used to conduct the analysis.

5.2. **Sample Network**. As stated earlier, the sample network used for this analysis is comprised of companies in the defense industry. I conducted a membership database comparison to identify a comprehensive population of the US members of the five defense industry trade associations.[24] The associations with the largest membership are the National Defense Industry Association and the Armed Forces Communications and Electronics Association. While it is difficult to classify many firms as US companies due to the multinational nature of the sector, there are approximately 2,600 US members of these and the other three relevant trade associations.[25] I selected ten of the largest weapons programs, either currently in production or planned for production, from which to derive a prospective sample from this

[24] Although the entire defense industrial base can be much larger than the membership of the five defense industry trade associations, this population boundary allows for identification of most technologically significant firms.

[25] The other defense industry trades are American Shipbuilding Association, Aerospace Industry Association, and Ship Building Council of America.

population of firms.[26] From this list of programs, a search of several publicly available sources identified six prime contractors (i.e., companies awarded contracts by the US Department of Defense), and more than 100 technologically significant subcontractors that produce major subsystems of the weapons. After identifying recent mergers and eliminating several foreign firms from the sample, I obtained a final sample size of 74 firms. I then derived the network of firms from the contractual ties created by partnerships on the major weapons programs. A valued directional graph can be generated from the number of contracts between firms and their prime and sub-relationships. However, for simplicity, the network was reduced to a simple bi-directional graph, based solely on the existence of a contract between the firms, as presented in Figure 1.

[26] The exact list of weapons programs that comprise the top ten in cost changes every year, based on production cycles. However, according to Department of Defense figures, the following programs are among the top expenditures: the C-17, F-22, F-35, F-18, and V-22 aircraft; Aegis, Virginia submarine, and Bush carrier naval systems; Army Future Combat System and Apache helicopter.

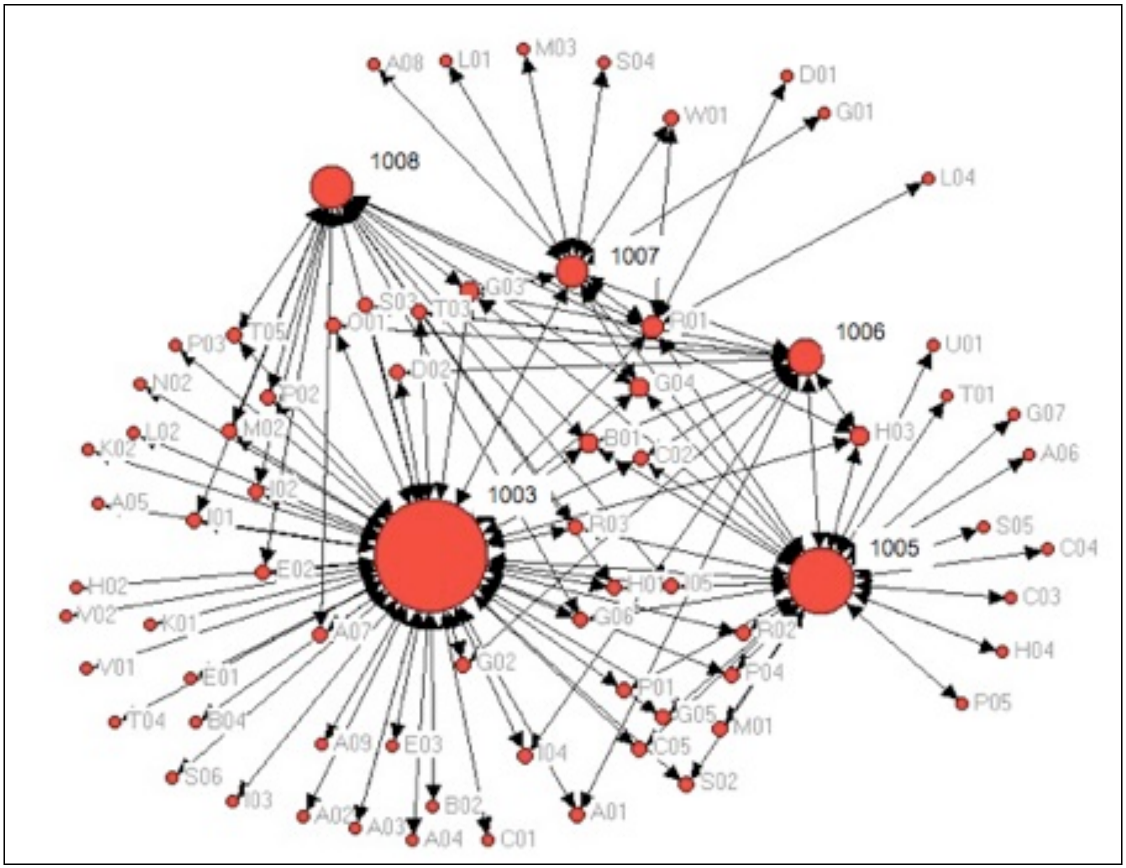

Figure 1: Sample network of defense contracting firms based on information-sharing relationships. Network exhibits scale-free characteristics.

An important characteristic of the resultant network structure was the high number of firms with a degree of one (i.e., only one contractual relationship in the network) and the few prime contractors with a very large degree (i.e., many contractual relationships). The histogram of degree per firm followed a power law curve that suggests that the underlying network has a scale-free nature. This initial finding is significant because it allows a researcher to expand the sample network into a network that represents the population in such a way that it contains the same relational properties (Barabasi 2003). As long as it is not necessary to specify the identity of every node, the general relationship between firms can be scaled. In other words, there is strong theoretical evidence that the analysis undertaken with this sample can be conducted on a network approximating the entire population identified previously. Moreover, any representative sample size between this and the full population of defense contractors, or perhaps a larger population than that which comprises the membership of these particular trade associations, should follow a similar structure. This preliminary finding suggests that this work can be applied more generally across the larger population in this sector, and perhaps to other sectors. It also helps overcome one of the shortfalls of mechanistic models, as identified earlier by Lopez-Pintado and Watts (2008).

Finally, the particular structure of this social network may significantly influence the decisions the firms in this system make about cyber security investment. Assuming that the vast majority of interactions occur through the prime contractor, or "knowledge integrator," the prime and its subs could be expected to have much greater knowledge of the investment decisions of fellow contractors on the same projects than they have of others' actions. The situation where all those working on the same project are expected to have insight into the decisions of others on that project leads to an extension of the basic IDSI model that I call "two-hop" vision.[27] In other words, the actors do not incorporate the investment decisions of those with more than two degrees of separation from them when calculating the external risk. It is important to note that this extension only changes the perception of the potential amount of system-internal risk created by others in the system who are not investing. In fact, it is possible that firms are so myopic and/or guarded in their investment decision that they may only share information with those to whom they are directly connected contractually. In this extension where the agents are maximally myopic, although the actors are in a system that includes 74 firms, the perception of security risks for many of these firms reduces immediately to a two-player game. For example, approximately 50 percent of the firms in the sample would consider only one other actor—the prime contractor with which they are sharing sensitive data—when calculating their risk from attack. This reduced ability to discern the investment decision of others reduces the complexity of the investment decision confronting any particular firm when estimating externally generated risk. Some researchers suggest that this restrictive amount of information-sharing is common in critical infrastructure sectors (see La Porte and Metlay 1996; Prieto 2006). However, the inability to

[27] The recommendation to include this extension of the model was provided to me by an anonymous review of the article being submitted to the International Journal for Critical Infrastructure Protection.

account for the investment decisions of the larger system may lead to a false sense of security in mixed-equilibrium states. In other words, a decision to invest in security measures may be ill advised, if there is a strong probability that the security measures will be ineffective against attacks that are launched on the firm from within the system—for example, socially engineered attacks through the firm's partners, against which its firewalls are largely ineffective. Nevertheless, firms may not accurately perceive the true level of this risk and may still invest in security measures.

5.3. **Agent-Based Model**. The model used in this analysis explores the potential decision-making behavior of defense firms within the sample network displayed in Figure 1. Analyzing the actual security investment decisions of the firms contained in this sample would require access to several forms of proprietary data from each firm. Furthermore, to obtain longitudinal results, the analysis would have to occur over a time period of several years. To overcome these limitations, this analysis employs an agent-based model. Because of firms' unwillingness to disclose details of their security investment, an agent-based model approach is particularly advantageous, as it allows for key parameters to be estimated within appropriate bounds but still be heterogeneously endowed to the agents, as would be expected in an empirical instance. The approach also allows me to consider the interaction of firms within a network—an impractical task for mathematical models.

Most agent-based models are constructed in an object-oriented computer programming language. The agents typically have two important components, attributes and behaviors. Attributes are encoded in *instance variables* and describe parameters such as an agent's state (e.g., whether it is investing in cyber security) or what it knows. *Methods* describe agents' rules of behavior, such as how they make investment decisions. In addition, the agents interact in an environment. To analyze the network's impact on the functioning of the model, I use two environments for this study: a fully connected environment, and the scale-free, empirically based network explained in the previous section. The agents in this model represent the decision-makers in the networked firms that are responsible for making cyber security investments. Agents who calculate their investment decision based on having full information of the others' decisions are considered to have perfect vision of others' actions. The basic IDSI model is then extended, using the network as described earlier. First, agents will be given two-hop vision, which relaxes the strict assumption of complete information but in a way that is influenced by the interaction network. Second, the agents become myopic and only consider the actions of others in their one-degree network neighborhood.

Based on the IDSI model equations, the significant attributes for the agents in this study are as follows:

Agent Parameters

c_i = Cost of investing in security to a level that defeats attempts at cyber espionage

L_i = Loss of critical information from successful espionage

p_{ii} = Probability of a direct, successful espionage attack on the firm

p_{ji} = Probability of an successful attack that occurs from within the interaction network

- Network neighborhood (number of other agents at a certain distance from the agent, such as one or two degrees, or "hops")
- Investment state (to invest or not invest)

Agents are heterogeneous, in that values of c_i, L_i, and p_{ii} differ across agents. Model parameters specify the mean values for the distributions that the model uses to select values of these agent attributes. For example, at model construction, the user specifies the mean (and standard deviation) for the distribution of investment costs, and then the model selects c_i as the investment cost of agent *i* by drawing from this distribution. This convention was necessary to analyze the model's response to a parameter sweep of the probability of system-internal attack, p_{ji}, while holding other parameters within realistic bounds. Similar to c_i, L_i, and p_{ii}, the model selects p_{ji} for each agent by drawing from a normal distribution; it is the mean of this distribution over which I performed the parameter sweep.[28] Note that for a particular agent, the probability of indirect attack (p_{ji}) is the same for all of its neighbors. Therefore, if an agent has three neighbors and one of them is not investing in cyber security, it does not matter which is not investing because the agent assumes the same risk of attack emanating through all neighbors.[29]

Based on consultation with cyber security experts and a review of industry reports,[30] the parameters were assigned using normal distributions with the following mean and standard deviation values:

Variable	Generating Distribution
$\boldsymbol{c_i}$	N ($1,000,000, $100,000)
$\boldsymbol{L_i}$	N ($50,000,000, $5,000,000)
$\boldsymbol{p_{ii}}$	N (0.4, 0.01)

Security investments can vary widely. For this research, it was assumed that all actors initially have some form of security in place. However, the current measures are assumed to be insufficient to counter a concerted cyber espionage attack. The binary choice becomes whether to invest at a level that

[28] There is no reason to expect that these parameters are truly normally distributed. The convention is only used to introduce heterogeneous behavior within realistic bounds.

[29] In other words, the risk from each other agent to which an agent is connected is the same. This convention was necessary to generate a less complex decision algorithm for the basic model.

[30] There are several ways for a company to secure its cyber enterprise from contracting the mission to developing in-house expertise. The estimates for this analysis were arrived at by discussing potential solutions with Symantec cyber security program sales and with Greg Rattray, Chief Internet Security Advisor for the Internet Committee for Assigned Names and Numbers.

safeguards against a concerted attack or to invest at a lower level (potentially no further investment). The loss from an attack could also vary widely. For this research, a value was chosen that approximates a fraction of the value of a weapons program over an investment period. Empirical data regarding the probability of successful intrusions that would result in catastrophic loss to the victim is not available. Therefore, the mean probability for a direct attack, p_{ii}, was set at 0.4, based on a recent report by data breach investigators at Verizon (Baker et al. 2009). While holding these parameters constant, the probability of a system-internal attack originating through any non-investing agent, p_{ji}, was varied from 0 to 1 to create a comparison when introducing extensions being assessed in hypothesis 1A.

In addition to the agent parameters, there are rules that govern agent interaction. The agents simultaneously make security investment decisions for each iteration of the model, according to the interdependent security payoff algorithms of the Kunreuther and Heal model.[31] Specifically, if an agent has n_i neighbors not investing in cyber security, the agent's external risk (x_i), expressed as the expected amount of dollars lost to a system-internal attack, is defined as:

$$x_i = L_i * \sum_{k=1}^{n_i} p_{ji} * (1 - p_{ji})^k \qquad (1)$$

[31] See Heal and Kunreuther (2005) for a complete presentation of the payoff matrix according to a two-person game.

An agent then calculates total risk (r_i), expressed as the amount of dollar loss expected due to not investing in cyber security, by:

$$r_i = p_{ii}(L_i - x_i) \tag{2}$$

Note that the greater the system-internal risk (created by others who do not invest), the lower the incentive to invest in cyber security, because this investment only protects against direct attacks. As stated earlier, if an agent has a high expectation of system-internal attacks against which they cannot successfully defend themselves, it makes little economic sense to make a large investment against direct attacks. Therefore, an agent invests only if the total cost of investing (c_i) is less than the total risk (r_i).[32]

In the current model, the behavior of the agents is algorithmically determined by the following:

<u>Interaction Rules</u>

- Identify how many others in your network neighborhood have not yet invested in security.
- Calculate the system-internal risk created by neighbors' decisions not to invest.
- Calculate the total risk, given the uncontrollable, system-internal risk.
- Determine whether the risk from not investing is less than or greater than the cost to invest.
- If the cost is less, then decide to invest. If not, then decide not to invest.
- Once all agents have made this decision, all agents update their state simultaneously.[33]

[32] For a derivation of the equations used to generate r_i, see Kunreuther and Heal (2003).

[33] Simultaneous state-changing was a convention employed to simplify the model. This is not a necessary limitation for agent-based modeling. Several other different state-change techniques, such as random action or sequential changes, may be employed in future versions of the model.

- Repeat the above process until no agent wishes to change his or her state.

Since Heal and Kunreuther (2007) identified the cost of the risk externality as the significant limiting condition, agents choose to invest in security when the inequality, $c_i < r_{i,}$ is true. All agents begin in the 'not investing' state. In an effort to avoid path dependence, all the agents make decisions based on a complete survey of the other agents, and they then change state simultaneously. This rule allows for a deterministic calculation of system-internal risks during each interaction period. Without this rule, any one agent would not be able to accurately estimate this risk during any investment period, regardless the interaction space, as it would be constantly changing.

5.4. **Incorporating Additional Extensions to the Model**. The inclusion of network based interaction spaces was explained previously. The next extension to consider is an endogenous consideration of the risk from a direct attack. One could assume that attackers will shift resources to focus on the most-weakly defended in an effort to break into the system as easily as possible (changing p_{ii}). Or, once in the systems, the attackers will look for those with which the victim most frequently interacts to expand the attackers foothold (changing p_{ji}). In effect, there are several ways to relax the assumption that the probability of an attack on any actor does not change in relation to investment decisions. However, it can also be argued that agents have limited ability to perceive their changing risk in the absence of continual attacks. Therefore, the extension I employ to make risk endogenous is related to p_{ii}. In this case, the agents use the same information they obtain regarding others' investments to estimate an increased likelihood of an attack directly against them. In this case, the agents assume their risk of a direct attack increases as the number of investing neighbors increases. Mathematically, the endogenously determined probability of a direct attack is given by:

$$p_{iinew} = p_{ii} + (1 - p_{ii})(K / N) \tag{3}$$

Where K neighbors in neighborhood size N (potentially the entire system) invest in security. Given this equation, the probability of a successful attack nears 1 as the calculating agent becomes the last in their interaction environment to invest.

The last extension of the model introduced to assess hypothesis 1A is the introduction of behavior that does not appear rational according to the decision-making rules. This extension could represent any reason that the agent would choose the opposite choice from the one expected based on the model's decision rules. The agents may be confronted with other immediate priorities for their funds, they may have inaccurate information on any of the parameters, or they may have no capacity to make a realistic assessment of their trade-offs. Since the decision being modeled here is binary, this is a simple extension to include. I simulate the non-rational behavior by forcing a certain percentage of agents to choose the opposite choice once they have made their otherwise rational investment calculations. It is important to consider that the non-rational decision from the investor's stand-point may be actually beneficial to them or to the system. When one agent makes a non-rational decision to invest in security measures, it may induce others to do like-wise. Then in T_2, the same actor may be induced to make a rational decision to invest since its neighbors have already done so. In other words, 'non-rational' may not equal 'bad' in the investment decision process.

To test hypothesis 1B, no changes to the interaction rules were required. Instead, the model is instantiated with a specified number of agents beginning in the "investing" state. The model is then run with no further constraints on investment decisions to observe if the specified coalition is successful at tipping the remainder of the system to a state of full investing or if the coalition collapses because it is insufficient to influence system-wide behavior. Before any of the extensions can be incorporated in the model to test hypothesis 1A and 1B, the model must first be tested in a basic form to ensure it can generate the game-theoretic predictions of the basic IDSI model.

5.5. **Docking the Model**. The agent-based model was first tested with a pooled risk environment, where all agents have perfect vision, to "dock" the model with the mathematical IDSI model. Docking entails aligning the two models to determine if the agent-based variant can produce the phenomena anticipated by the mathematical model, for example, tipping, cascading, and the relevant equilibria. With an initial endowment of parameters as defined above and agents with perfect vision, all significant predictions of the basic mathematical model were obtained. Specifically, a non-investing, full investing and, a mixed equilibrium were all achieved. These results were sustained over several runs of the model at varied levels of p_{ji}. Figure 2 depicts these results graphically.

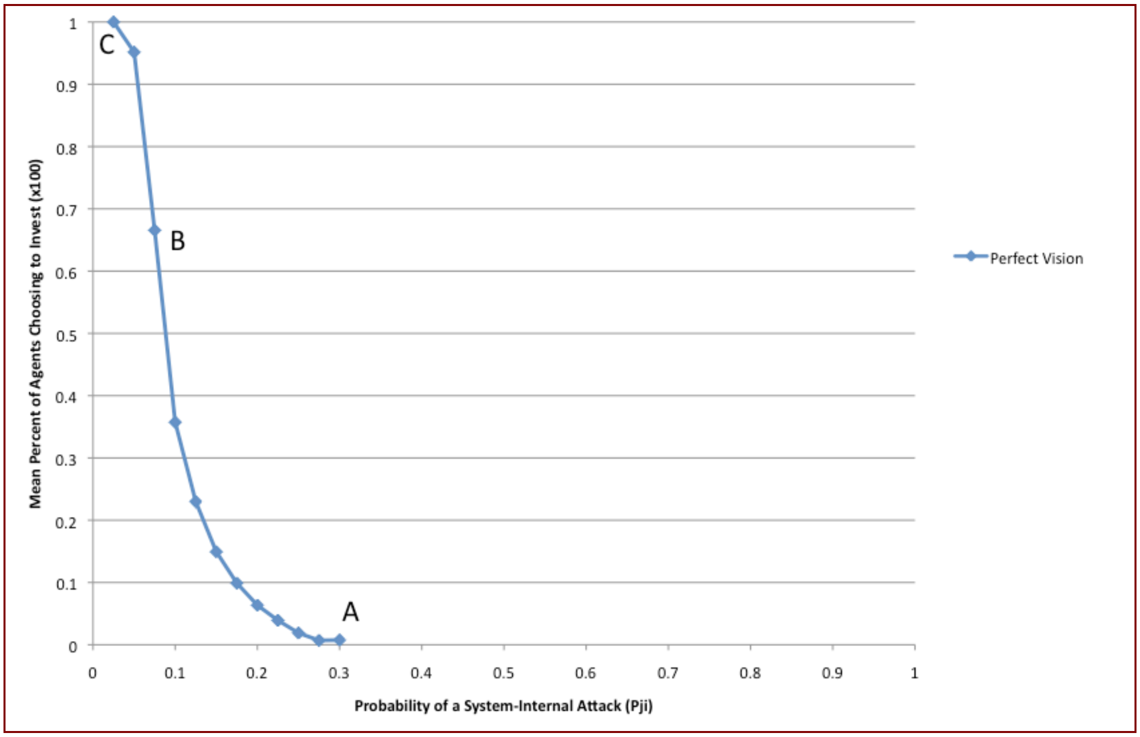

Figure 2: Changing equilibrium values of system-wide investing when agents have perfect vision regarding others' investment decisions.[34]

It is easiest to read this chart from right to left as the desired behavior of system-wide investing *increases* when the probability of a system-internal attack *decreases*. In other words, the situation improves from the public good standpoint as p_{ji} gets smaller. For example, Point A at $p_{ji} = 0.275$, and all points to the right of Point A, depict equilibria where no agents choose to invest in cyber security measures.[35] Adjusting p_{ji} over a range of 0.25 down to 0.1 produced both limited investing decisions at equilibrium and some

[34] In this and ensuing graphs, the X axis of this chart represents the mean value of p_{ji} with a normal distribution about the mean.

[35] In Figure 2 and subsequent figures depicting the same information, the curves were discontinued when the system mean reaches either 0 or 1. However, the values are continuous in all cases.

cascading security investments by the agents. Cascading to higher levels of mixed equilibria occurred lower at $p_{ji} \approx 0.10$ down to 0.075. The steep curve from 0.1 to 0.05 shows that the model was very sensitive to altering the probability of system-internal attack over this range. Tipping to an equilibrium state where the entire system was motivated to invest during every run did not set in until $p_{ji} \approx 0.025$. When the probability of an attack emanating through others in the system dropped to 0.025 (Point C in Figure 1) or lower, the entire system quickly chose to invest independent of other agents' decisions (i.e., they did not need to be tipped by others' investment decisions).

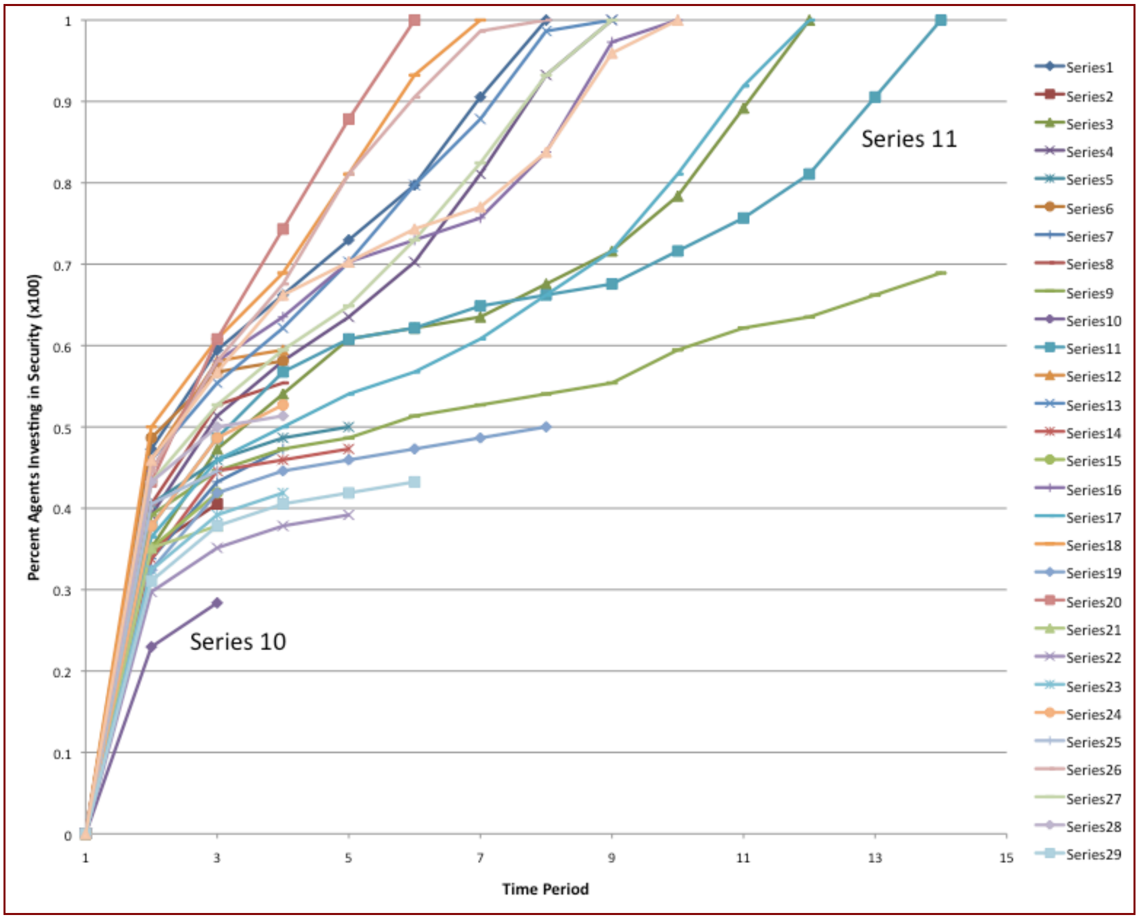

Figure 3: Model runs when p_{ji} is 0.075. Agents have perfect vision.

Figure 3 shows the results of the model that were averaged to obtain Point B in Figure 2. This figure demonstrates the occurrence of mixed equilibria, cascading behavior, and tipping to full investment during runs of the model when p_{ji} was set at 0.075. For example, the agents making investment decisions in Series 10 (purple diamond curve) reached an equilibrium at T_3 in which less than 30 percent of the agents chose to invest. After that, no agents desired to change their investment decision. On Series 11, however, the decisions of early movers enticed others to follow suit. The result was that the system cascaded all the way to full investment by T_{14}. The behavior of the model's agents, given these particular parameters, conformed well to the predictions from the basic IDSI theory. According to the basic IDSI theory presented by Heal and Kunreuther, their theory predicts a state of no investing when the risks against which an actor cannot defend are too high. The theory predicts conditions in which mixed states will occur and a risk region in which all actors can be expected to invest in security measures. The theory also showed mathematically how decisions to invest by some actors can influence others to invest as well. All of these conditions occurred in the docked model.

Once the agent-based model was successfully docked to the mathematical model, the extensions to test hypothesis 1A and 1B were introduced into the system. The resultant changes in the agents' investment decision behavior are presented in the next chapter.

6 Analysis and Findings

6.1. **Introduction.** In this chapter, I explore hypotheses 1A and 1B and present findings regarding the agents behavior after introducing each extension. After the agent-based model was successfully docked, the model was instantiated using a step-wise process to introduce the first two extensions—network influences and endogenous risk to test Hypothesis 1A. The potential effect of the network was further sub-divided into a two-hop view and myopic view as explained in the methodology. For each extension, the model was run for 30 iterations at incremental levels of p_{ji} to obtain an average level of investment at equilibrium (when the agents no longer wanted to change their states, given others' states) for both extensions. When equilibrium levels of investment are sustained over time, and at similar levels of risk as in the basic model, meaning that there is not an unrealistically low or very high probability of attack required to achieve equilibrium, then the hypothesis is determined to be valid. The introduction of non-rational behavior requires a slightly different approach. In this case, the model was altered to allow agents to act for 100 ticks (time periods) in each instantiation of the model. In this extension, the model was only tested with parameters that were expected to produce mixed equilibria when all agents acted rationally.[36]

Hypothesis 1B tests the effect of introducing an initial coalition of investors. The first step to analyze the influence of a coalition is to determine appropriate collections of actors (central or peripheral) and the number of firms to be included. Several different sizes of coalition can be tested, but for this analysis the initial coalition is comprised of the prime contractors. Prime contractors are the focus for the initial coalition because they are an identifiable sample on which to focus public policy. To test the influence of an initial coalition on the investment decisions in the system, the model is run at varying levels of p_{ji} without and then with the initial coalition while holding all other parameters constant. As identified earlier, Kunreuther and Heal consider this parameter a principal feature of the IDSI model. If others are not investing and the firm is exposed to a high risk of attack against which it cannot defend itself, there is little incentive to invest otherwise. The initial coalition's impact is considered critical when the coalition induces the system to tip toward full-investment at a level of p_{ji} that is both statistically higher than without a coalition, and realistic based on industry reports. In

[36] Non-rational behavior means that the model will never reach a perfect equilibrium where no agents will be discouraged to change their investment decision. Therefore, there is no value in testing the model in states where rational agents would all choose to invest or not invest.

other words, the system may not tip without a critical coalition until p_{ji} is below 0.01 and then tip with a critical coalition at a level of 0.02. While the difference may be shown to be statistically significant, a p_{ji} of 0.02 is not realistic according to industry reports that show the threat of an attack from within a system of business partners to be above 0.3 (Baker et al. 2009). As will be demonstrated, another option to induce tipping is to increase the size of the initial coalition to influence their behavior at expected levels of system-internal risk,

6.2. **<u>Analysis of Hypothesis 1A</u>.** The first step in analyzing hypothesis 1A was to introduce the networked interaction environment. As explained above, the model was instantiated using a modified interaction environment (but otherwise with the same parameters as with the docked model), for several runs over a range of values of p_{ji}. The model successfully reached equilibrium in a manner consistent with the docked model and at realistic values of all parameters. However, depending on the network interaction assumption used to extend the model, two-hop or myopic vision, the alteration of the interaction environment to a scale-free network structure had substantially different effects on the agents' security investment behavior.[37] Agents with two-hop vision did not display an investment

[37] In fact, capturing the average level of investment at equilibrium conceals the fact that runs at each level of p_{ji} could have widely varied results as well. Refer to Figure 3 for a depiction of how differently the agents may behave collectively during each series.

behavior that was markedly different from those with perfect vision. However, myopic agents, interacting in the empirically-based, scale-free network environment achieved a 100 percent investing equilibrium at much higher levels of externally generated risk than those acting with either perfect or two-hop vision. Based on the given model parameters, full system investing among myopic agents occurred at levels of p_{ji} of 0.45 and below. However, the network of agents appeared much more resistant to tipping and cascading than was observed in the docked model. Figure 4 below depicts these results graphically. In Figure 4, the average percentage of agents choosing to invest when the system achieves equilibrium is plotted according to the probability of an attack originating from within the system. The resistance to tipping amongst the myopic agents is demonstrated by the gradual slope of the light-blue-X curve compared to the other two curves. The following sections contain a detailed explanation of the results presented on this graph.

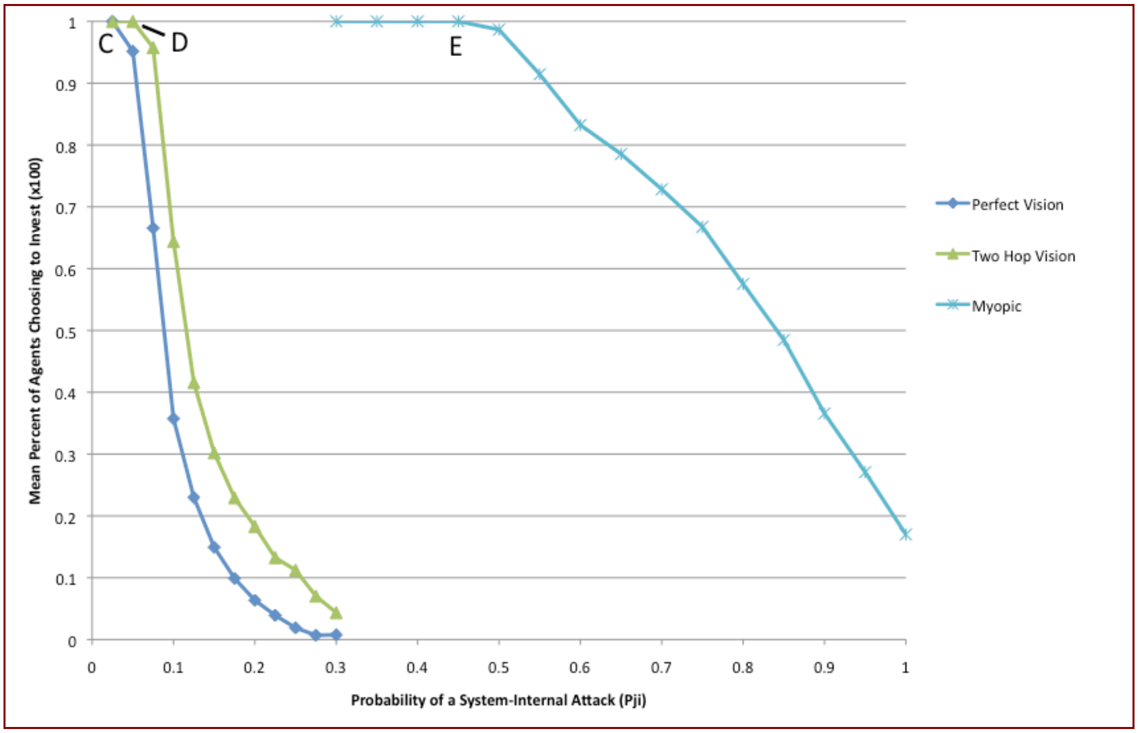

Figure 4: Adding network-based interaction space to model. Agents have either "two-hop" vision or they are so myopic they only consider the investment decisions of their immediate neighborhood.

6.2.1. **Effect of a Scale-Free Network on Investment Decision Equilibrium**. The dark-blue-diamond curve in Figure 4 tracks the investment decision equilibria investment decisions when agents are endowed with perfect vision (i.e., they perceive an environment of pooled risk and can see all others' investment decisions). As stated in the discussion on docking the model, unless p_{ji} is 0.25 or lower, no agents choose to invest at equilibrium. At a p_{ji} of 0.25, an average of only 1.8 percent of the agents choose to invest. It is not until p_{ji} is as low as 0.075 that the mixed equilibrium reaches an average of 66 percent investing. However, the steeply sloping portion of the curve reflects the fact that cascading frequently occurs at a p_{ji} of 0.05, and the system quickly tips to an equilibrium where all choose to invest when p_{ji} drops to 0.025 (point C in Figure 4).

The green-triangle curve in Figure 4 tracks the investment decision of agents with two-hop vision. Point D, at a p_{ji} of 0.05, depicts the equilibrium at which all these agents choose to invest for this extension of the model. From a p_{ji} of 0.075 to approximately 0.3 mixed equilibria result. This behavior is not substantially different from that of agents with perfect vision. As the graphs show, agents with two-hop vision behave only slightly differently than those with perfect vision over the entire range of full investing, to mixed equilibrium, to an equilibrium at which no agents invest. This behavior most likely reflects an important characteristic of scale-free networks. The fact that several actors have a high degree of connectivity with many other actors means that any one actor is no more than a few degrees from any other in the network. Therefore, even though the agents only have vision that extends two hops (degrees), that degree of sight encompasses almost the entire network and closely approximates perfect vision.[38]

[38] Future research could assess the influence of different sizes of networks or those that more closely reflect random graphs. It is likely that agents interacting within a randomly connected network would have a less extensive vision of the entire system within two hops.

The light-blue-X curve tracks the investment decision of myopic agents—those who can only see their immediate neighbors in the network. Based on the parameters for this model, Point E, at a p_{ji} of 0.45, depicts the equilibrium at which all the agents with this trait choose to invest. In fact, the agents achieve a mean of 98 percent investing at p_{ji} of 0.5, well before the point at which agents with either two-hop or perfect vision choose to invest this broadly. Clearly, the greatly limited perception of risk led to a much greater incentive for the myopic agents to invest at higher levels of probability of attacks emanating from within the system. As stated earlier, this effect results from the fact that any one actor within the network does not consider the risk potential of other actors that are not in its direct network neighborhood (within one degree of separation). Additionally, in the scale-free network, most actors on the periphery are only connected to one other central actor in the network. If a central agent is investing at a level sufficient to thwart attempts at catastrophic cyber espionage, the perceived security externality faced by myopic agents on the periphery is zero. Therefore, these peripheral agents will invest quickly, as long as the cost to do so is less than the expected loss from a direct attack. Based on the model's assumption that threats can flow freely within the network once they have penetrated one actor's outer defenses, these agents could be dangerously discounting the threat from within the system. However, if the threat actors do have difficulty transiting from one defender to the next, then the defenders' security investments may be more cost-effective.

6.2.2. **Increased Resistance to Cascading and Tipping**. Although the myopic agents interacting on a network reached an equilibrium of full-system investment at higher levels of system-internal risk, the scale-free structure caused some agents to be more resistant to cascading and to tipping toward the 100 percent investing state. As explained above, many actors in a scale-free network may only account for externalities created by one other actor. As such, they are often prone to invest at a higher level of system-internal risk at time step one (T_1). This behavior accounts for the more gradual slope of the light-blue-X curve in Figure 4. Considering the parameters used in these instantiations, mixed equilibria begins at levels of p_{ji} as high as 1.0. However, as also stated earlier, the probability of indirect attack must drop to 0.5 before the vast majority of remaining agents have decided to invest as well. So why can't the myopic agents who begin to invest at higher risk levels cause the system to cascade and ultimately tip the rest of the agents to invest at an equally high level of system-internal risk? The reason lies, again, in the scale-free nature of the network. Now the investment decision must be considered from the point of view of the agents both on the periphery and in the center of the network. While the actors on the periphery must only account for the decision of one other actor in the network, the central actors must consider the system-internal risk posed by the non-investing decisions of significantly more actors. As stated, some peripheral agents determine that it is beneficial to invest as early as T_1. However, many other peripheral agents, and specifically the central agents, are reluctant to do so. Until all but one of the agents on the periphery have chosen to invest, the investment decision of the remaining agents on the periphery and the central agent are not comparable. In other words, central actors are confronted with much greater risk levels. Therefore, the central actors resist investing in security much longer than the remaining actors on the periphery. This resistance hinders the ability of the system to tip toward an equilibrium in which all myopic agents have chosen to invest. Again, if the original assumptions of the model regarding transfer of risk are correct, this creates a dangerously broad range of probabilities where mixed investment states are prevalent.

6.2.3. **Endogenous Risk.** The second step in assessing hypothesis 1A was to introduce changing risk into the model. The model was instantiated using a modified risk calculation according to equation 3, but otherwise with the same parameters as with the docked model, for several runs over a range of values of p_{ji}. This extension was tested in all three, interaction landscapes—perfect, two-hop, and myopic vision. The model successfully reached equilibrium in a manner consistent with the docked model and at realistic values of all parameters. Based on the modified risk calculation that agents undertook according to equation 3, their investment behavior did not change markedly except in the case of myopic agents.

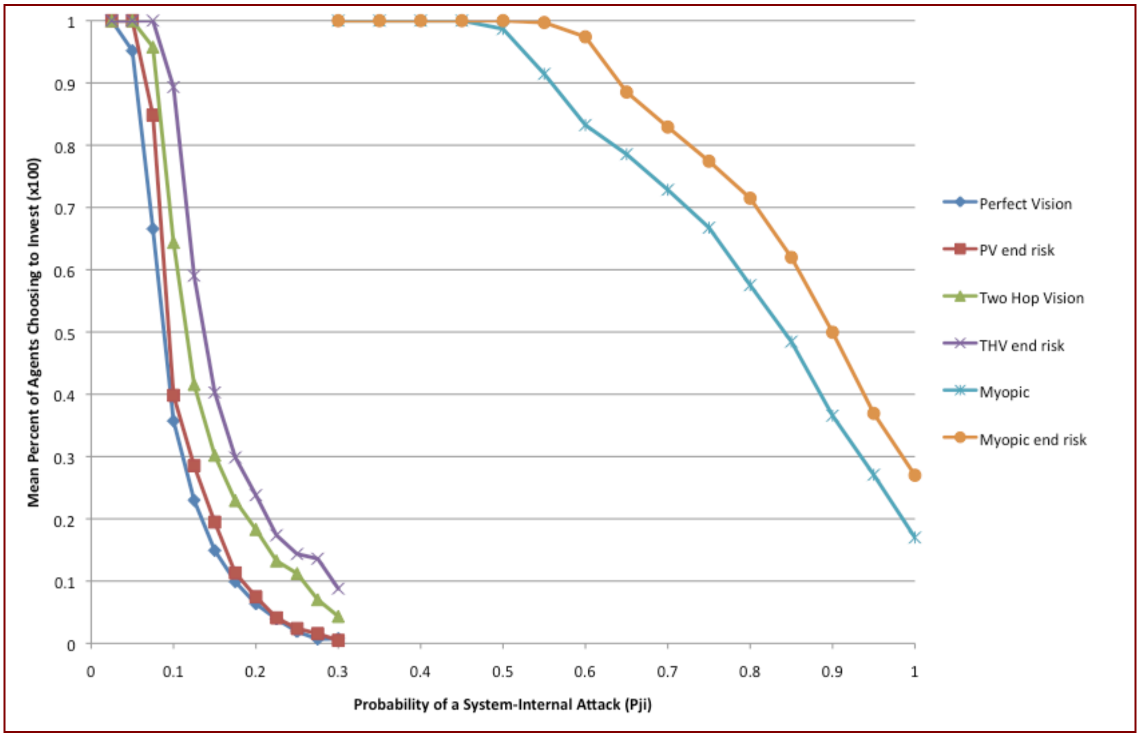

Figure 5: Adding endogenous risk calculations to the model. Agents expect that the risk of an attack directly targeting them will increase as neighbors invest in security measures. The myopic agents are most influenced by this alternation.

According to the modified risk calculation, the agents perceived that their risk from a direct attack increased as a function of the number of their neighbors investing in adequate security measures. In other words, the expected risk of a direct attack increased from the originally estimated probability of 0.4 and approached 1.0 as the number of similarly unprotected neighbors diminished to zero. Figure 5 depicts the influence of endogenous risk on the model. As demonstrated by the additional curves in Figure 5, the difference in behavior appeared to be most marked in the case of the myopic agents. The orange-circle curve, representing agents with myopic vision who have modified their assessment of risk, suggests that, at all levels of p_{ji}, 10% more agents choose to invest at equilibrium than myopic agents who have not internalized risk in their investment decision calculations. On the other hand, adding risk to the other two interaction environments shows much more marginal results. Only small bands of p_{ji} values correlate to significant differences in investment, specifically when p_{ji} is between 0.075 and 0.125. This difference in the agents' responsiveness to internalizing risk should be expected based on the algorithm used. Since the increase in p_{ii} is directly influenced by the fraction of the neighborhood that invests, smaller neighborhoods, as in those surrounding myopic agents, will result in more rapid increases in p_{ii}. The rapid rise in p_{ii} will result in more immediate decisions to invest. But what does it mean for the behavior to be different in this case compared to the other interaction environments? It depends on the true nature of the threat landscape. For example, if the actual probability of an attack emanating from within the system is at 0.55 or higher, and the other parameters are accurate representations of the system, then internalizing risk will encourage a sufficient number of actors to invest in adequate cyber security measures. In general, the only conclusion that can be drawn from this extension is that including adaptive risk in the model did not cause the agents to behave in an unexpected fashion. On the contrary, the agents were more motivated to invest in security measures in all forms of interaction space and over most values of p_{ji} for each case

6.2.4. **Non-Rational Behavior**. The final step in assessing hypothesis 1A was to introduce non-rational decision-making. The simplest way to introduce non-rational behavior was to force the agents to switch their binary choice from the rationally determined one at each time period. To accomplish this extension, a user-controlled parameter was added to the model where I could choose any level of non-rational behavior to be induced randomly amongst the agents. For example, I could select a level of non-rational behavior at 10 percent of agents. The agents would finish determining their investment decision based on the parameters and interaction rules explained previously, then a randomly chosen sample of 10 percent of the agents would switch their decision to the opposite choice. This extension represents any reason for which the agent would choose the opposite state from the one expected based on the model's decision rules.

Figures 6 thru 9 depict some of the effects of introducing non-rational behavior into the model. Figures 6 and 7, show the behavior of agents endowed with perfect vision and faced with a probability of 0.075 for attacks emanating through the system. These parameters are the same as those that generated Point B in Figure 2. These parameters also correspond to the agents whose investment behavior is depicted in Figure 3. Figure 6 shows a fairly stable fraction of investors fluctuating between 34 and 52 percent that continues over 200 model time periods. The reader will notice that the percentage of agents investing in security fluctuates between 34 and 52 instead of being near 65 percent as expected by the mean value at Point B in Figure 2. The answer is found in Figure 3. In those instances where the system does not tip to full investing, the fraction investing was actually somewhere between 0.4 and 0.6. Since this instantiation of the model never cascaded above those bounds, it would seem indicative of a series in Figure 3 where the system never tipped, such as Series 10.

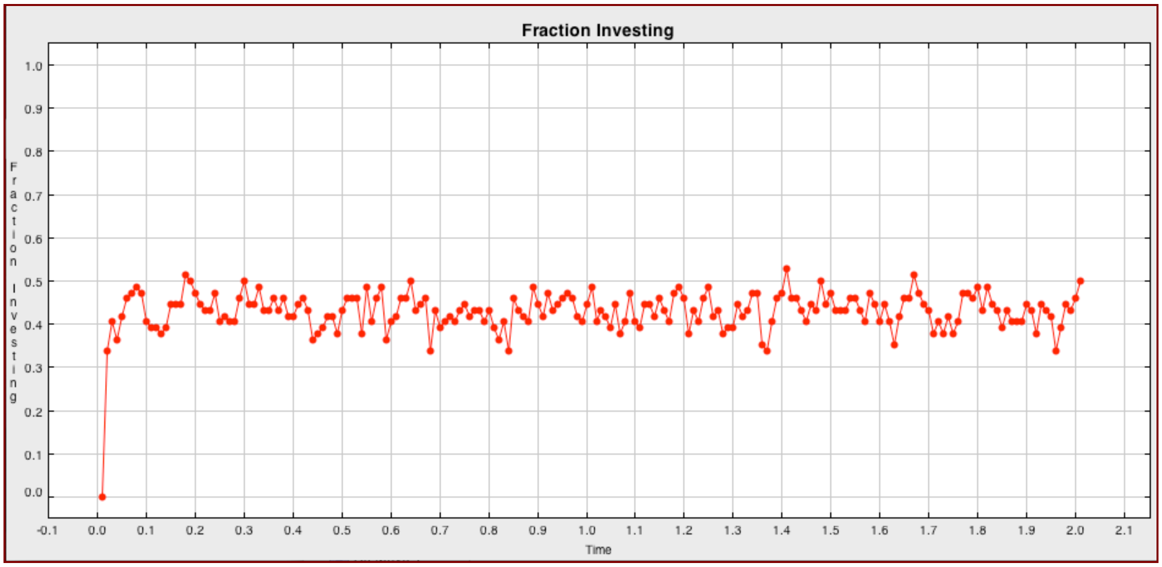

Figure 6: Agents endowed with perfect vision but 10 percent make non-rational investment decision during each time period.

Figure 7 depicts a different result, but one also anticipated from the cascading behavior of some agents shown in Figure 3. After a long period of stability near 50 percent, the system cascaded to a state where 95 percent of the agents invest in security measures. In fact, given that 10 percent of the agents were not behaving rationally in each time period, it is likely that this run would have otherwise tipped to full investing. Even when it dipped to under 80 percent at T_{93}, the system still returned to a much higher state of investing by T_{98}.

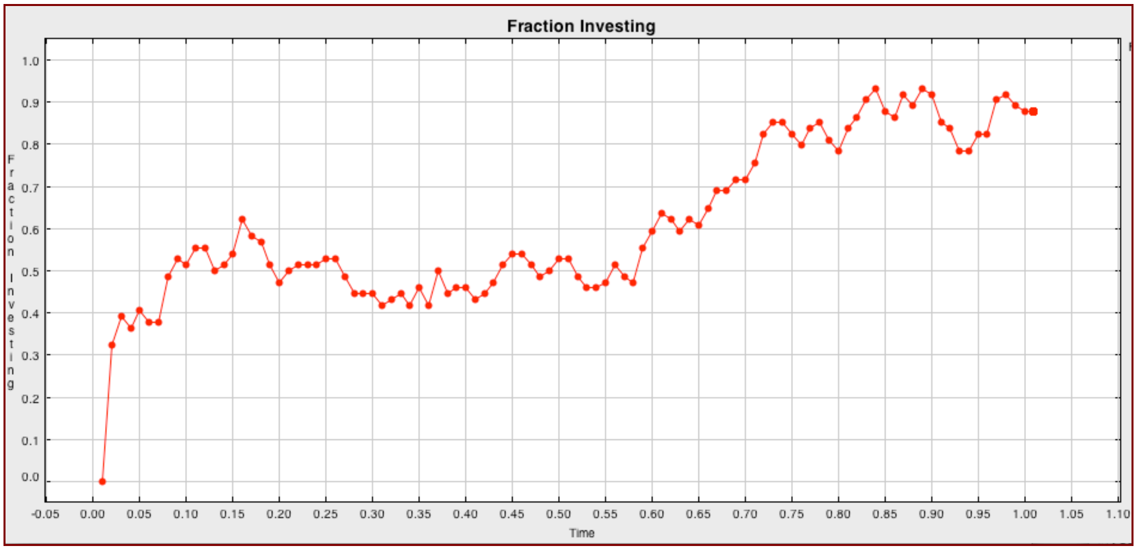

Figure 7: Agents endowed with perfect vision but 10 percent make non-rational investment decision. Evidence that cascading can still occur.

The tests I conducted under these parameters established that the model could produce generally stable results consistent with the basic theory in the case where up to 10 percent of the agents make non-rational investment decisions. The rational behavior parameter was next altered such that 30 percent of the agents chose the non-rational investment decision at each time period. All other parameters were the same as those used for the runs depicted in Figure 6 and 7. The results of this model alteration are depicted in Figure 8. While the greater amount of non-rational behavior caused the level of investing to fluctuate more severely than in the system depicted in Figure 6, this result continued to be within acceptable bounds. Most importantly, introducing this greater amount of non-rational behavior did not create substantial instability in the system. In other words, at the macro level, the system of agents continued to behave in a manner comparable to the docked system.

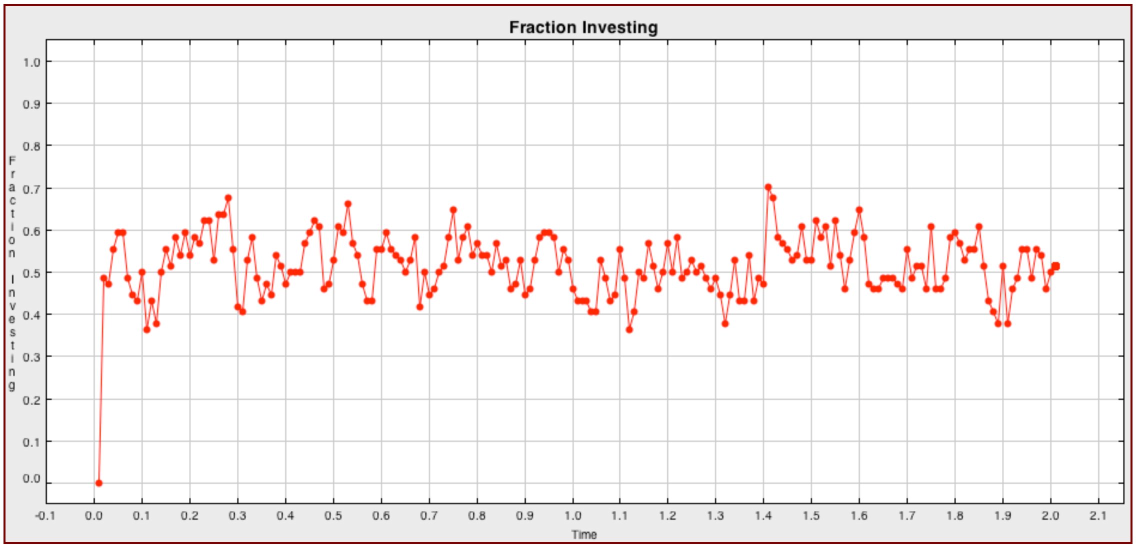

Figure 8: Agents endowed with perfect vision but 30 percent make non-rational investment decision. The system continues to function in a stable manner, yet oscillates more than in the case of 10 percent non-rational decisions.

With this initial finding established, I moved to explore the impact of non-rational actions in a model with the full extensions—myopic agents and those who have adaptive risk assessments. As shown in Figure 9, the model still demonstrated a great degree of stability over 200 time periods. After the exploratory run shown in Figure 9, the model was instantiated and run an additional 30 times for 100 time periods each. In all runs, the model maintained the same amount of investing, approximately 90 percent of agents choosing to do so, during each period. These results support the theory that non-rational behavior may not necessarily mean behavior detrimental to the system as a whole. In fact, non-rational behavior from an individual perspective may be rational, or at least beneficial, from a collective perspective.

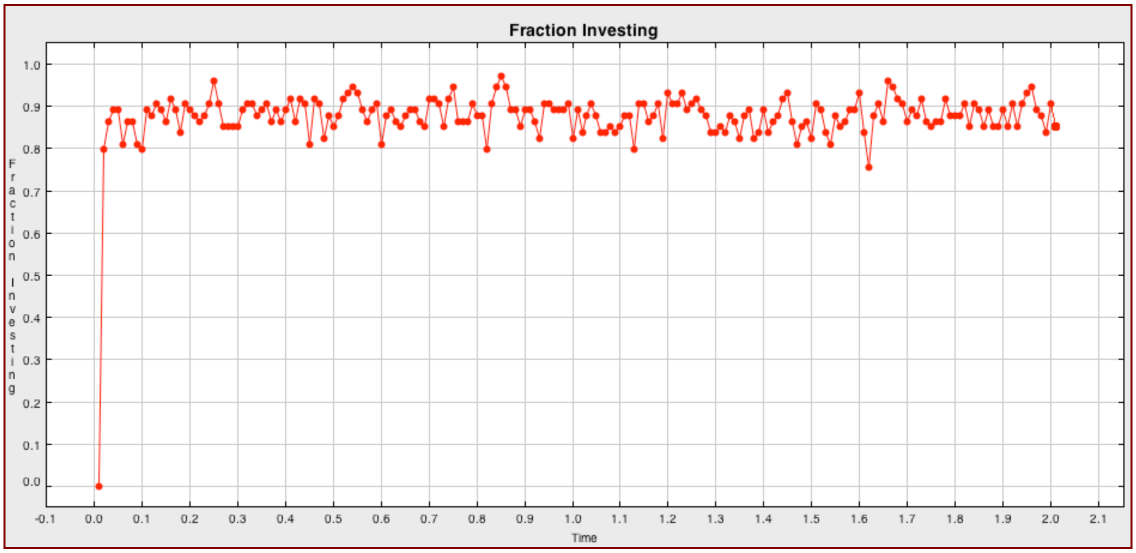

Figure 9: Agents endowed with myopic vision and endogenous risk but 10 percent making non-rational decision.

The goal of testing hypothesis 1A was to establish that the IDSI model could be adapted to a situation that approximate a sector of critical infrastructure. The ultimate goal of employing the IDSI model is to support public policy measures designed to improve security investments in an interdependent infrastructure sector important to national security. One measure to motivate the necessary level of security investment could be to influence a coalition to invest under conditions in which most would not choose to do so. The purpose of this initial coalition would be to induce a sufficient fraction of the system to follow suit in invest in security when they would otherwise not do so without their behavior being coordinated in any manner. Hypothesis 1B explores the influence of an initial coalition comprised of central actors in specific interaction networks.

6.3. **Testing Hypothesis 1B: Impact of an Initial Coalition on Investment Decisions.** One of the important characteristics of the IDSI model is that it postulates the existence of critical coalitions that can tip the system to an equilibrium in which all actors invest. Such a coalition could tip the system under conditions that would otherwise result in a mixed equilibrium or an equilibrium in which no actors choose to invest, even though all actors would be better off investing. Theoretically, the problem is only one of coordination (Ostrom 1998; Schelling 1960). If the coalition encourages enough others to invest, the externalities could eventually be reduced to such a level that the benefits for all would outweigh the cumulative costs. Unfortunately, it is very difficult to ascertain empirically the sufficient composition of this critical coalition in any given system of actors. The problem is no easier in an agent-based model. Both the size and composition of a critical coalition is dependent on the endowment of all parameters of all agents, which varies across model runs. However, it is possible to study a specific initial coalition in the agent-based model in order to explore the general conditions under which it may be considered a critical coalition. The size of the coalition, or other parameters can then be easily altered in an agent-based model to explore other ways to influence the behavior that emerges in the system.

For this study, I assessed the critical coalition theory using the two network-based interaction landscapes. I only used these two landscapes for two reasons. First, the model results for the agents with two-hop vision have been sufficiently similar to those of agents with perfect vision. Second, an interaction space in which no actors play any discernable role, such as in the case of pooled risk, does not provide any insight for where public policy could be applied. For example, if all agents are expected to have similar threat landscapes and interaction rules, there are no easily identifiable central actors and therefore no suggestion as to where to influence behavior. Any collection of actors could be chosen as the initial coalition.

Since the prime contractors are a discernable collection in the sample network used for this research, it is more insightful to begin the analysis with them. To test the influence of an initial coalition within the contract-based interaction network, all the agents in the network who had a degree of six or higher were assigned an initial state of investing. This alteration of the initial conditions resulted in a coalition representing all six prime contractors in the system as depicted in Figure 10. For this instantiation, the agents in the coalition were not forced to remain in a state of investing beyond T_1. In other words, the agents were free to disinvest during any subsequent period if the system-internal risk was too high to make investing cost-effective in subsequent periods.[39] This convention could simulate a situation in which all prime contractors met at T_0 and agreed to invest without enforceable consequences for changing their decision in a later period.

[39] While the agents could be forced to invest for longer periods, it would be more efficient from an enforcement perspective if the agents are encourage to invest adequately with minimal effort at coordination.

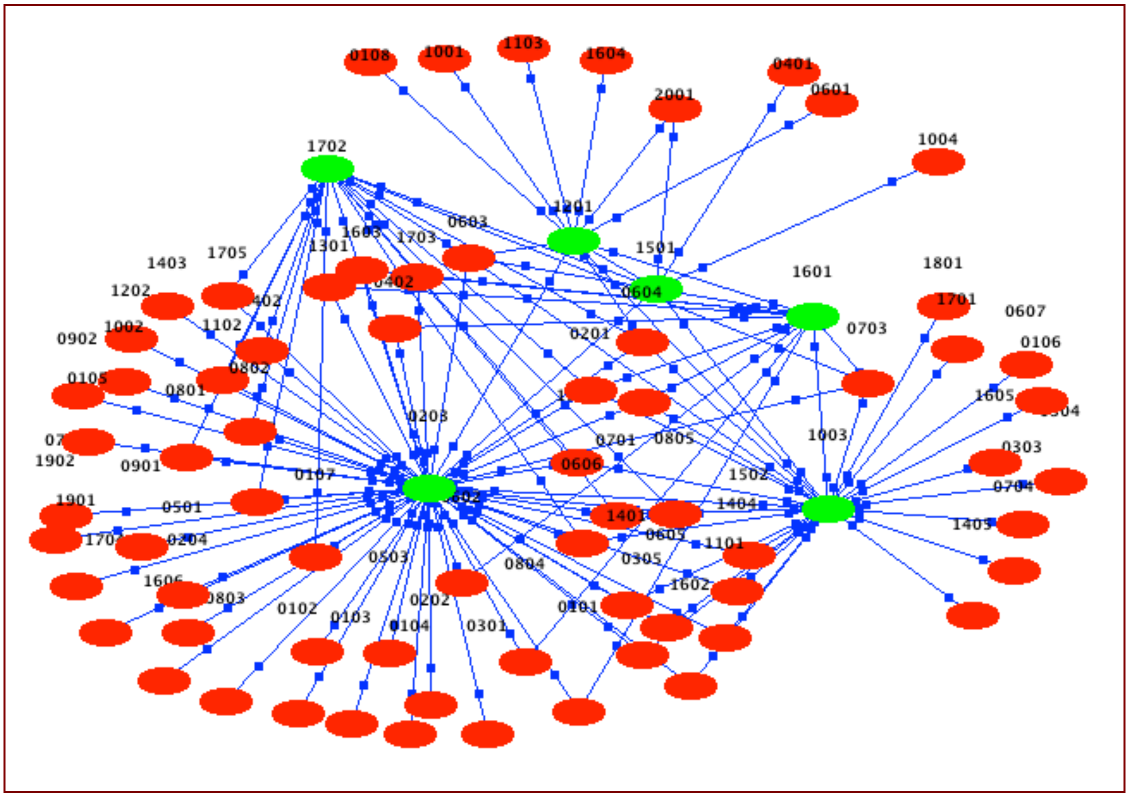

Figure 10: Initial coalition of all prime contractors.

6.3.1. **Initial Coalitions Among Rational Agents with Two-Hop Vision.** The coalition was first introduced to the system of agents endowed with two-hop vision who acted in a rational manner.[40] For this analysis, the agents were endowed with endogenous risk calculations and otherwise the same other parameters as in earlier analyses. Instantiating the model using agents with two-hop vision and an initial coalition of the six central actors led to disappointing results. With all parameters equal, an initial coalition of six

[40] The problem of coalitions among non-rational agents will be discussed in a subsequent section.

agents had no discernable effect on the investing behavior of the system at all levels of p_{ji}. Depicting the resulting curve on any of the figures would be unhelpful because it would lie directly on top of the curve representing the system without an initial coalition. Based on this initial finding, the size of the initial coalition was increased to find one that demonstrated a measurable impact at any level of system-internal risk. It was not until a coalition of all multiply connected actors (with a degree of 2 or more) was established that any insightful results were obtained. The resulting coalition was comprised of all primes and 31 other firms that participated on multiple projects. This initial coalition comprised half the actors in the system.

The purple-X curve in Figure 11 represents the investment behavior of the agents with two-hop vision and endogenous risk considerations when there is no initial coalition to influence investment behavior. The light-blue-plus curve to its right represents the introduction of an initial coalition of 37 actors. Based on the results depicted in Figure 11, the introduction of a coalition of half the actors—under the conditions specified for this extension—still seems to have a minimal effect on the decision-making behavior of the agents at p_{ji} values of 0.25 or higher (Point F). However, the coalition appeared to have a substantial influence on the system when the expected probability of a system-internal attack was at or below 0.225 (Point G). The coalition can be said to be a critical coalition, one that causes tipping to full investing, when the p_{ji} is at or below 0.175 (Point H). An additional convention was employed to increase the influence of this coalition. The interaction rules were adjusted to require the security investment decisions to last three subsequent time periods. However, this extension only prolonged the inevitable collapse.

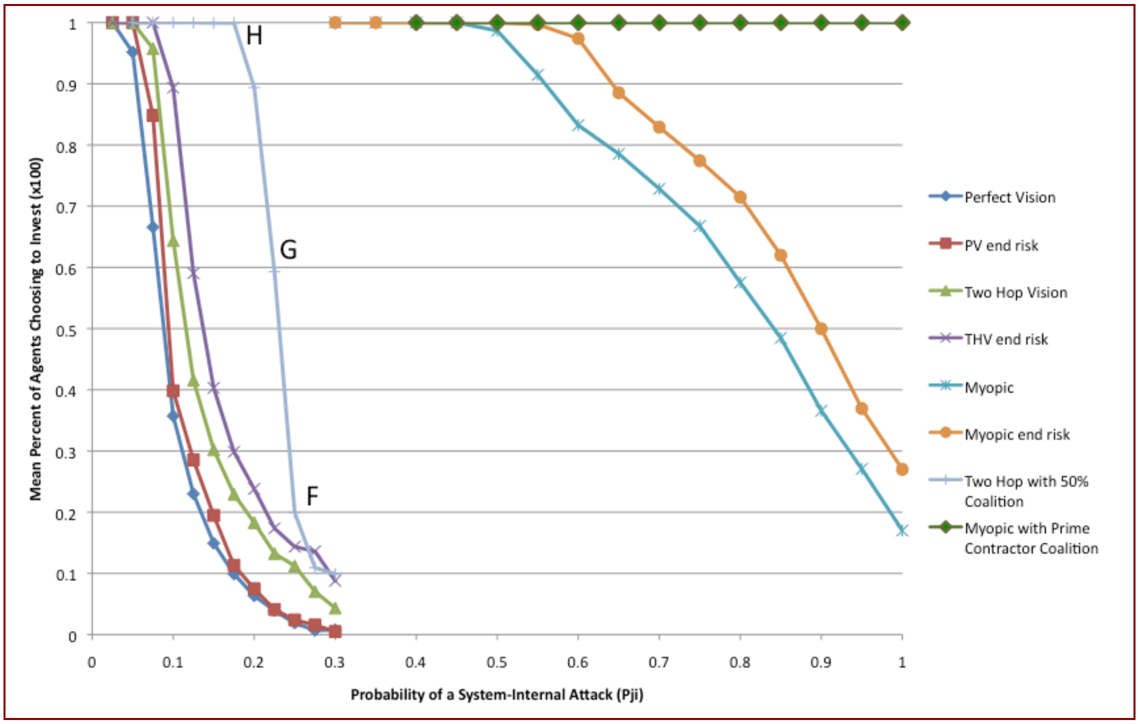

Figure 11: Model instantiated with initial coalitions. Initial coalition of half the system has minimal effect when agents have two-hop vision. Coalition of six central actors is critical for all values of p_{ji}.

Agent-based models can help us understand how this collapse can occur. This collapse phenomenon is depicted in Figure 12. This graphic represents the behavior of the agents with two-hop vision, a value of $p_{ji} = 0.2$, and the presence of an initial coalition of half the agents. In all series, the level of investment starts at 50 percent (due to the presence of the initial coalition) and increases until T_4. After T_4, there is no requirement for the initial coalition to maintain its mandatory level of investment. If insufficient numbers of other agents had been induced to invest by this period, the central agents changed to a state of non-investing. After this, the entire system quickly followed suit and chose not to invest in security measures. In such situations, the vast majority of the system may choose to disinvested by T_9.

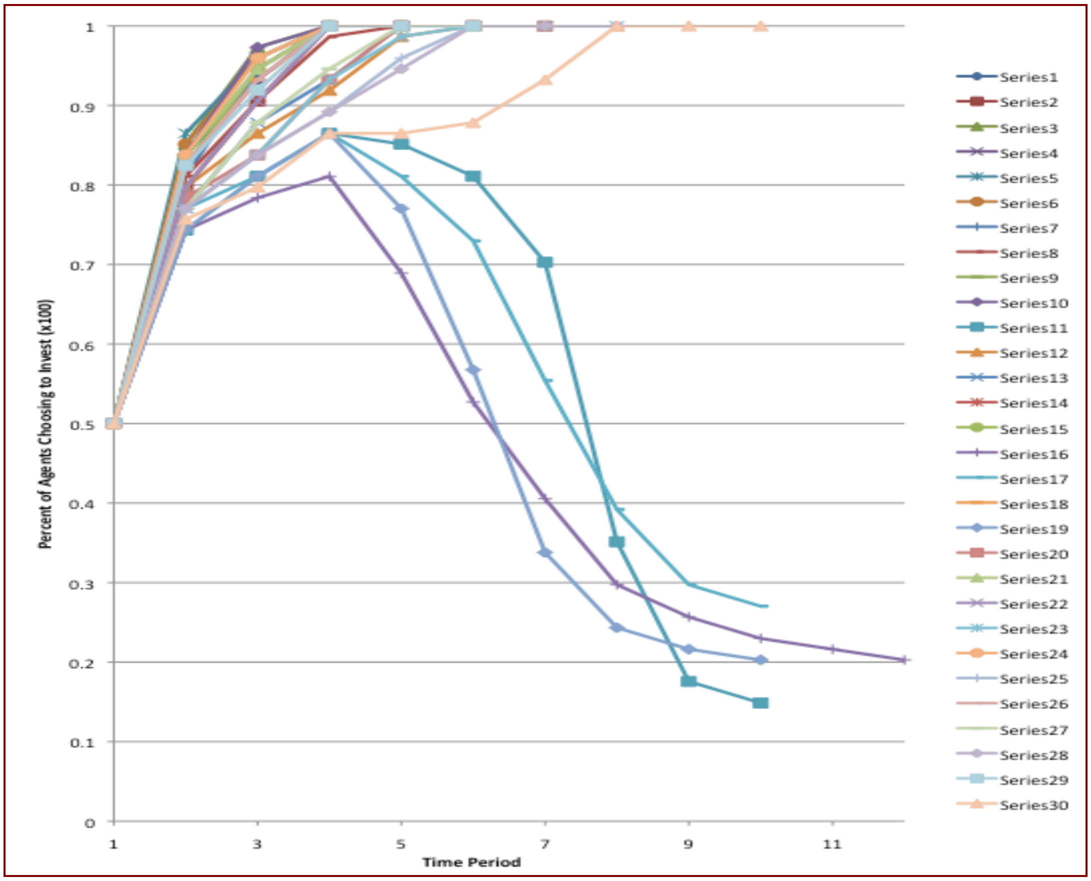

Figure 12: The collapse or success of an initial coalition.

Unfortunately, these results do not meet the criteria established for Hypothesis 2B. First of all, the coalition is considered critical for only very low levels of p_{ji}, 0.175 and below. This level of probability of an attack from within the system is not realistic based on industry estimates that it is higher than 0.4. Secondly, the hypothesis requires that the initial coalition be a small subset of the entire system so as to provide a focus for public policy. However, a coalition of half the actors in the system could not be considered small enough to inform policy in an effective manner. If the actions of one half the relevant actors must be coordinated, the costs to do so would be prohibitive absent a legal requirement for the action. Even with legal requirements to do so, effectively inspecting the investment would be another substantial challenge. Therefore, under these conditions, coordinated action of a small coalition of firms in this system does not appear effective to tip the system toward full when faced with significant, cyber threats.

6.3.2. **Initial Coalition Among Rational Agents with Myopic Vision**.

The dark-green-diamond curve in Figure 11 depicts a very different result when the initial coalition of prime contractors is introduced to a system of myopic agents. In this situation, the membership and size of the coalition have greater significance. Influencing the central actors to invest at T_1 means the perceived, system-internal risk is immediately lowered to zero for the vast majority of peripheral agents. As a result of this large reduction in system-internal risk throughout the system, almost all the peripheral agents changed their state to investing immediately at T_2. In fact, the rapid move to invest on the part of the peripheral agents discouraged the central agents from disinvesting during the subsequent periods and kept the coalition from potentially collapsing.[41] Since the system tips to a state of full investment across the entire range of $p_{ji,}$ the coalition of six central actors appears to be a critical coalition under all conditions specified in the model for myopic agents.

The ability of the coalition of central actors to encourage a state of full investing at high levels of p_{ji} is important given the states of mixed investing equilibrium among myopic agents that would otherwise dominate at $p_{ji} > 0.5$. As stated earlier, these mixed-equilibrium conditions are based on the fact that myopic agents undervalue the risk from system-internal attacks. The myopic agents undervalue this risk because they do not account for the investment decisions of others in their CI sector, but outside their immediate interaction neighborhood. According to the IDSI model, any non-investing actors in the system but outside the neighborhood still pose a risk to all actors in the system. Therefore, the faulty risk perception of myopic agents may lead to a decision to invest that is neither privately nor publicly beneficial if this incomplete level of investing cannot effectively thwart cyber

[41] Preliminary trials conducted with just one agent removed from the coalition suggests that there is a real potential for the coalition to collapse if tipping does not occur quickly.

espionage intrusions that propagate through the system. It is only when the system reaches a state of full investing that the reality of the risk matches the perception. At this point, there is no longer a system-internal risk that the myopic agents could under-estimate.

Returning to Hypothesis 1B, we can conclude a different result that presented in section 6.3.1. If the agents can be assumed to be myopic in their interaction space, their behavior in the model suggests that an initial coalition of a small collection of central actors can tip a system toward sustained levels of full investment. This coalition can be considered critical even when the threat of a security breach emanating from within the system is very high.

6.3.3. **Critical Coalitions and Non-Rational Behavior**. The introduction of non-rational behavior presents an additional challenge to the ability of any initial coalition to influence the system to tip to investing. Introduction of an initial coalition implies that the decision to invest can be coordinated and then enforced, either through self-regulation or other means, for a sufficient length of time to induce tipping in the system. If the agents cannot be expected to commit to a decision to invest in an initial period, it is difficult to determine what size coalition can be considered critical and to assess how the system will respond in subsequent periods. Even if the initial coalition can be expected to commit to investing in the first period, earlier tests of this model have shown that the system will have difficulty tipping to full investment if there are non-rational decisions not to invest in any subsequent period. The full impact of non-rational decisions cannot be predicted a priori, but it can be assessed with the agent-based model if one additional convention is added to the parameters.

The influence of non-rational behavior can be analyzed if the agents are required to commit to their investment for enough periods to allow the system to tip to a state of full investing before being affected by non-rational behavior from any agents. I instantiated the model using the same parameters as in the test for myopic agents making endogenous risk calculations (brown-circle curve in Figure 11) to assess this extension in a way that can be compared to previous results. As in the previous tests, an initial coalition of all six prime contractors was introduced at T_0. To introduce non-rational behavior, I directed a random selection of 10 percent of the agents to choose the opposite decision once they had completed their investment decision calculation. This is the same technique I employed earlier to assess non-rational behavior. However, as with an earlier test of initial coalitions, one additional convention was employed to allow the initial coalition to be established sufficiently to influence the system.

In this test, the agents who invested each period were directed to maintain their investment for three subsequent periods. In other words, all agents were faced with an equal probability of making a non-rational decision (10 percent), but once they had made the decision to invest, they maintained it for a total of four periods. As a result of this parameter, the initial coalition of investors maintained their investment for a total of four periods from instantiation. They were then free to choose not to invest, or maintain their investment, in subsequent periods. All other agents were also imparted with this investment "lock-in" one they chose to invest. This convention is not unrealistic. It could represent some form of mandatory action directed at the initial coalition in early periods. It could also represent the fact that those who choose to purchase their cyber security-related capital equipment, instead of leasing equipment or hiring a cyber security firm each year, will most likely maintain their capital investment for several years before re-considering their investment decision. The results of the test using these parameters are shown in Figure 13.

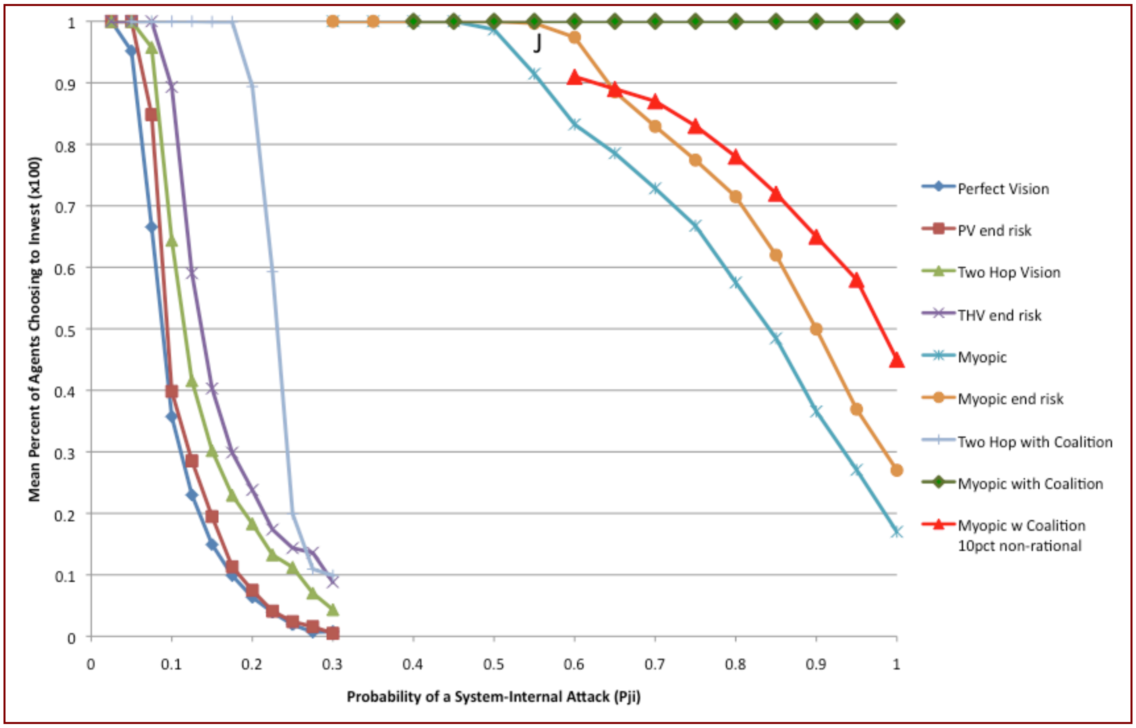

Figure 13: Non-rational behavior causes the initial coalition to collapse at high values of p_{ji}.

The red-triangle curve in Figure 13 represents the impact of non-rational behavior on the system. So that I could compare the results of this test with previous configurations, I conducted thirty runs of the system at each level of p_{ji}. During each run, I allowed the system to make investment decisions for 100 time periods. After 100 periods, I determined the average level of investment for the system from T_4 to T_{100}, the periods after the tipping influence of the initial coalition. Then I calculated the mean of the means over thirty runs at each level of p_{ji} and plotted this value on the chart to generate the red-triangle curve. The results are informative at values of p_{ji}

above 0.6.[42] As predicted, the system was not able to maintain a state of full investing at any level of p_{ji} above 0.7. Unfortunately, the level of investing continued to decline as p_{ji} neared a probability of 1. The position of the curve above the other two curves for myopic agent behavior shows that the coalition did have some influence on overall investing levels. However, there is no indication that the coalition could be considered a critical coalition for values of p_{ji} above 0.7 since the amount of investing in stable conditions was well below 100 percent.

Effective provision of the public good of national cyber security, under these parameters, cannot be achieved. If the goal requires a level of system-wide investment near 100 percent at levels of p_{ji} at or above 0.7, non-rational behavior, significantly impacts the coalition's ability to influence behavior sufficiently at any level. Returning to hypothesis 1B, we must conclude a different result than when myopic agents act rationally according to the IDSI model. These results suggest that, when non-rational behavior is introduced, coordinated action directed at the six central actors cannot be expected to tip the system toward full investment in situations where the probability of a system-internal attack is significant. In this case, a "significant" level would be considered to be one above that in which the system would be induced to

[42] At values of p_{ji} below 0.6, it appears that the results are worse than in the system without non-rational behavior and no initial coalition. However, it is difficult for the system to maintain levels of investing above 90 percent under any conditions when 10 percent are always making the non-rational decision.

invest in the absence of an initial coalition. For example, at levels of p_{ji} of 0.5 and lower, the system of myopic agents who internalize direct risk calculations can be expected to cascade to full investment without an initial coalition (Point J in Figure 13). Introduction of a critical coalition would be expected to be of value to this system of actors at any higher level of p_{ji}. However, accounting for the fact the system of 10 percent non-rational agents will not be expected to maintain investment levels above 90 percent, introducing a coalition of the six prime contractors will not induce a sufficient level of system-wide investment at p_{ji} above 0.6. In effect, the initial coalition has no significant impact, given the model's current parameters, beyond a short range from p_{ji} of 0.5 to 0.6.

These findings have implications for the basic model. If the non-rational behavior depicted in this model can be expected to occur in empirical settings, then we must question the ability of an initial coalition to lead to substantial levels of system-wide security investment given any system parameters or interaction space.

6.3.4. **Discussion**. In this research I have used an agent-based modeling technique and introduced an empirically-based environment to explore the interdependent security invest model. The agent-based model showed that, under the modeled parameters, the basic tenets of the IDSI model can be observed in a simulated environment of many agents making interdependent security decisions. The results of introducing an initial coalition to influence system-wide behavior were mixed. This research demonstrated that, under conditions derived from empirical data, it can be very difficult for a small initial coalition to significantly influence the behavior of the rest of the agents such that the entire system tips to a state of full investment in security. However, extending the basic model to explore potentially myopic investment behavior led to result to different behavior. In this case, a small coalition of initial investors could tip the system to an equilibrium condition of full investment as long as all agents behaved otherwise rationally according to the basic model. Non-rational behavior in the investment decision again led to a situation where it was difficult to sustain a full investing equilibrium in the system.

Of course, the extensions employed to test the above hypotheses take us well past the basic IDSI model. Therefore, it would be logical to consider other potential extensions that may counteract the influence of non-rational behavior as I have modeled it. For example, there is no role for trust in the basic IDSI model. As Ostrom (1998) has stressed, next generation models of bounded rationality should explore the theoretical role for trust and its role in solving social dilemmas. Since trust has been demonstrated to play an important role in several studies, perhaps the idea of trust can either counter act the negative impact of non-rational decisions (give the agent the benefit of doubt and not follow suit in the short term) or even counter act non-rational behavior (convince an agent to invest regardless any structural or random pressures to do otherwise). In addition, I did not incorporate the behavior of the sector-specific agency to coordinate and influence cyber security investment decisions. As the federal agency designated by HSPD-7 to oversee the security of this CI sector, the DOD has designated organizations to help coordinate investment actions and help to mitigate the adverse impacts of non-rational behavior (ASD(NII)/DOD CIO 2010).[43] These and other factors can be explored in future modeling exercises.

Before presenting comprehensive conclusions and discussing the public policy implications of this research, I will next turn to the second collective action challenge of private sector involvement in cyber security—sharing information regarding cyber threats and response actions. In Part III, I will present the methodology used, and analysis of results, for investigating the cyber security information-sharing network in the electric power sector.

[43] I will elaborate on DOD's potential roles for DIB cyber security in the final chapter when I discuss policy recommendations.

Part III

Cyber Security Information-Sharing in a Complex Infrastructure Sector

7 Introduction and Prior Work[44]

7.1. <u>Overview</u>. The horrible oil spill in the Gulf of Mexico reminds us that our addiction to fossil fuels has become costly in many ways. In recognition of the significance of energy to our national security, President Obama's has initiated steps to transform the nation's energy infrastructures (Executive Office of the President 2009). For the electric power sector in particular, there has been a move to modernize the infrastructure so that our energy use becomes significantly more efficient. This greater efficiency will require a transformation of the electricity monitoring and control systems in such a way that demand and supply can be monitored at ever increasing points to a much greater level of precision. Such innovations are components of what is coming to be called the "Smart Grid" (Morgan et al. 2009). But the very innovations necessary to achieve these goals of increasing energy efficiency also create potentially significant cyber security vulnerabilities. Historically, the electronic systems that monitored and controlled the various processes to generate and distribute electric power were proprietary systems on closed

[44] Substantial portions of Chapter 7 come from an unpublished working paper entitled, "Cyber Security Collaboration in the Electric Power Sector: Potential Research Agendas" submitted for partial course credit, PUBP 796, Dec 2009.

networks (Energetics Inc. 2006). To use them required both knowledge of unique protocols, and direct access to the control networks. With the move to IP-based systems and remote access capabilities, the challenge confronting hackers has been substantially eased. Now many of these control systems can be probed and potentially accessed from any point on the globe by anyone possessing a general knowledge of IT networking fundamentals. In addition, the increased interdependence in critical infrastructure means that several other critical sectors dependent on electric power will also experience increased vulnerabilities as a result. For example, petroleum, telecommunications, and water distribution all depend on reliable electricity supply (DOE 2007). Considering that this critical infrastructure sector has already shown itself to be a potential target of malicious actors, it will be important to address these issues before the technologies of the Smart Grid are widely implemented.[45]

Though innovations in the physical components of this CI sector are designed to improve national security by increasing efficiency, increased cyber vulnerabilities may have the opposite effect. Clearly private actor actions in this CI sector are as important to overcome these vulnerabilities in

[45] According to national intelligence experts, foreign hackers have gained access to the control system networks for the nation's electric power generation and transmission on at least two occasions (Harris 2008). In fact, Tom Donahue, a Central Intelligence Agency cyber-security expert who now works on the national security council staff, publicly acknowledged that hackers have penetrated foreign utilities and have even demanded ransoms, a form of cyber extortion (Harris 2008).

cyber security as those in the defense industrial base and several other sectors. As argued in Part I of this dissertation, two important actions that the private sector must undertake are increased security measures and participation in the cyber security information-sharing network. Though the power generation and transmission entities in this sector must contribute to both components of cyber security, the focus of Part III will be cyber security information-sharing network unique to this sector.   In this part, I will employ a case study approach to analyze the electric power sector owner-operators' motivations to share information vital to national cyber security. Understanding and improving information-sharing will become more vital as the nation moves to implement the Smart Grid.

Both the Department of Energy (DOE), and the Department of Homeland Security (DHS) recognize that innovations in the infrastructure to employ smart-grid technologies could further increase risks by introducing substantially more access and control points (Vijayan 2009). Several efforts have been undertaken by these organizations to address problems on several fronts to include the *Roadmap to Secure Control Systems in the Energy Sector* in 2006 and the recently released DHS *Strategy for Securing Control Systems* (2009b). The DOE and DHS sponsored Roadmap (2006) identified sharing of cyber security information as one of the major areas in which government and private industry must improve efforts in order to meet the challenge of securing the sector from cyber threats. According to the Roadmap, information-sharing between industry and government has been inadequate due to such factors as, "uncertainties in how information would be used, disseminated, and protected." Though information-sharing was identified as a primary goal in the 2006 *Roadmap*, a recent report by the Energy Sector Control Systems Working Group (2009) stated, "most information protection and sharing issues between the US government and industry have not been resolved."

One of the most unfortunate consequences of this continuing problem with information-sharing is that cyber security professionals at electric power sector operational facilities are not provided the necessary data to make a compelling case to management for investing in greater cyber security (DOE 2009). Greater investment in cyber security is another near-term, Roadmap milestone that cannot be accomplished without detailed threat information and data regarding effective defensive measures. Such information is important to help resource managers allocate effectively between competing priorities in electric power firms. Clearly, emphasis must be placed on improving information-sharing amongst the collection of organizations that provide electric power and those that are responsible for ensuring the overall security of the nation's critical infrastructure.

Chapter 7 will continue with a discussion of the current cyber security regime in the electric power sector and an analysis of the stakeholder communities. Several public and private organizations already play important roles in developing and implementing security measures to include procedures to disseminate and report cyber security data. In the final section of Chapter 7, I will review select works about the concept of inter-organizational collaboration from a network perspective. The intent of this review is to demonstrate the applicability of social networking theory to the public policy issue of cyber security in the electric power sector.

7.2. **Cyber Security Regime in the Electric Power Sector**. In the electric power sector, at least ten stakeholder communities are important to, or potentially benefit from, sharing information on cyber security threats and effective defense measures. Some stakeholders are specific organizations while others can be grouped as a collection of actors based on their similar characteristics and information needs. This section will begin by presenting the perspective of owner/operators (hereafter referred to as "operators") and other private sector actors, move to "in-between" organizations, and then to public agencies.[46]

[46] Although there are significantly more public-owned electric power generation organizations, private firms and cooperatives generate 85% of the nation's electricity (APPA 2007). Therefore, the initial stakeholder analysis does not identify federal government electric power production facilities as distinct stakeholders. In Chapter 8, I will show this to be a faulty assumption.

In the physical domains of land, air, and sea, where the front lines of defense are maintained by the nation's military and homeland security agencies, in cyberspace, the operators of critical infrastructure components must fill this role as national defender. Often the operators are the only ones who can see intrusion attempts on their cyber systems, or effectively monitor and assess their security efforts. As in other sectors where the effective monitoring or provision of services is dependent on control systems linked through cyberspace, the operators of electric power generation and distribution systems are the best positioned to identify potential attacks on their systems and gauge the attacks' impact. In fact, another challenging aspect of cyber security is that, unlike fences and security guards protecting a physical asset, the defenses in cyberspace are not visible to the casual observer. Neither industry organizations, federal agencies, nor the attackers can gauge the effectiveness of existing defenses unless an intrusion and attack on a control system is successful with visible results.[47] Ultimately, the electric power facility operators are also the only actors that can determine which security measures worked well for them, and which do not, based on previous intrusion attempts. Therefore, both information on the attacks being made against them, and the effectiveness of their defensive measures, are important items to share with the sector's stakeholders. Often the intent

[47] Even then, the intruder can only see each line of defense as it is encountered and therefore may not understand their chances of success at any point in time.

of an attack cannot be discerned until the information is fused with other intelligence to which federal agencies have access. Also, other operators would benefit from understanding the methods and tools of the attackers and the "best practice" defenses that may better secure their operations. Based on the information operators provide and the clear benefit they would receive from shared experiences and threat analysis, the operators play a pivotal role in cyber security for this critical infrastructure sector.

The next group of stakeholders is comprised of commercial vendors and control system suppliers. Vendors are the best positioned to understand the security features and potential vulnerabilities of control systems they have designed. Vendors also have the greatest understanding of the full-range of effects on system parameters and system functioning from successful attacks. The vendor may not be able to assess specific impacts at each installation, given that the systems are implemented in unique configurations, but the vendor does have the best overall understanding of potential impacts on operations (Energetics Inc. 2006). In addition, the vendor is motivated to ensure their products are as secure and resilient as possible. Therefore, they desire information on current attack methods, tools, and vulnerabilities that others using their control systems may have encountered (Rakaczky 2010).

The third group of stakeholders is comprised of industry organizations. Electric power industry organizations, such as the Edison Electric Institute and the National Rural Electric Cooperative, are included in this category. These organizations represent the interests of large constituencies in the sector as well as smaller organizations that do not have the resources to interact with legislators, regulators, and other federal agencies. Industry organizations have the ability to pool resources and generate sector-wide support for addressing issues like cyber security. They can set and support research agendas. In addition, they can maintain libraries of defense "best practices" and contribute to the development of cyber security standards. Importantly, they collect and analyze data on important industry issues to help members make smart investments (EEI 2009).

The fourth stakeholder, the North American Electric Reliability Corporation (NERC), straddles the public and private sectors. NERC is a self-regulatory organization, situated between the government and the owner-operators of the electric power sector. It is subject to the oversight of the Federal Energy Regulatory Commission (FERC) (NERC 2009). NERC is responsible for developing industry-wide security standards, to include those for sharing cyber security information, and submitting them to the FERC for approval. NERC's primary role regarding cyber security information-sharing is to manage the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The ISAC is the central industry hub for threat information on cyber threats to the commercial portion of the electric power sector. As implied by the name, the ISAC conducts analysis on threats and defenses then disseminates the information as appropriate (NERC 2008). In it's central position, the ES-ISAC is structured to receive threat and vulnerability information from the federal government, operators, vendors, and researchers. It can then promptly broadcast threat indications and analysis across the sector to support proactive defensive measures and to mitigate attacks (NERC 2008).

Turning to the federal government, the fifth stakeholder, the Department of Energy (DOE) is the sector specific agency responsible for oversight of security in the electric power sector (EOP 2003). To facilitate information-sharing and collaboration on security threats, DOE established the Energy Emergency and Assurance Coordinator (EEAC) system to share information among states, local governments, and the DOE Office of Electricity Delivery and Energy Reliability (DOE 2007). In its role as the sector lead for the federal government, DOE also receives threat information from government and private sector sources. The primary means by which DOE receives information from operators regarding cyber security issues is the DOE Form 417. Operators must submit this form any time there is an incident that has or may affect electric reliability. The incident can be cyber or physical. Based on these inputs, DOE disseminates threat and vulnerability analyses across the electric power sector and to research centers. Federal power management administrations, such as Bonneville Power and the Tennessee Valley Authority, also fall within the DOE enterprise. These organizations are most similar to the private sector operators regarding their power generation role. However, they do not have the same cyber security legal and information reporting requirements that private operators have.

The federal government's overall lead for coordinating infrastructure protection incident response across all critical infrastructure sectors is the Department of Homeland Security (EOP 2003). Since it's establishment in 2003, DHS has led efforts to improve cyber incident response to include creating the US Computer Emergency Readiness Team (US-CERT). Within US-CERT, DHS recently established the industrial control systems CERT (ICS-CERT) as the central fusion center hub for all industrial control system cyber security issues (US-CERT 2009a). ICS-CERT attempts to communicate directly with all sectors of critical infrastructure that are reliant on control systems to function. In the case of the electric power sector, the ICS-CERT receives information from operators and others to analyze threats then disseminates information back to all CI sectors to implement security measures. DHS, along with DOE, also communicates with vendors and research laboratories to improve products and develop software and hardware updates. DHS recently formed the Industrial Control Systems

Joint Working Group (ICSJWG) (US-CERT 2009a). This working group addresses control system cyber security within all critical infrastructure sectors. To focus specifically on the energy sector, DHS and DOE established the energy sector control systems working group (ESCSWG) under the Critical Infrastructure Partnership Advisory Council (Energetics Inc. 2006). This working group has been tasked to implement the roadmap for securing control systems in this sector. The ESCSWG is the body that made the earlier stated observation that little progress has been made in addressing cyber security information-sharing issues in the electric power sector.

The seventh stakeholder important to electric power sector cyber security is the Federal Bureau of Investigation (FBI). Since DOE and DHS organizations responsible for cyber security oversight have no law enforcement authorities, the FBI must be integrated in the cyber security regime for this purpose. Several years ago, well before the responsibility for critical infrastructure protection was moved to DHS, the FBI established the Infragard program as a partnership between the FBI and the private sector (FBI 2009). The program is designed to share threat information regarding cyber attacks and support the FBI's investigative mission. With its law enforcement authorities, the FBI can share threat information analysis with the federal government intelligence community. The FBI may also share specific, sensitive but unclassified threat data, and information for forensic analysis, when there is not a pending investigation (FBI 2009). Since only a limited number of private sector operators have the clearances required to receive highly classified information from the intelligence community, the information shared with industry is often not sufficiently detailed to influence cyber security measures at operator locations.

The eighth group of stakeholders, also within the federal government, is the national intelligence community (IC). Through the DHS Homeland Infrastructure Threat and Risk Analysis Center, IC organizations, such as the Central Intelligence Agency and National Security Agency, produce threat briefings for both federal agencies and private sector entities when events dictate (US-CERT 2009b). In order to produce this analysis, the IC also assesses information received from DHS, DOE, and the FBI to help direct intelligence collection efforts that can further support national cyber security.

Research laboratories comprise the next group of stakeholders. Laboratories can be private, public, and combined. For example, the Electric Power Research Institute, an independent non-profit, and the DOE Idaho National Labs, both conduct research dedicated to the cyber security problem (INL 2009). Research labs have a distinct advantage over operators due to their access to test facilities for cyber security measures. Since operators must ensure reliable delivery of electricity on a continual basis, they are not able to risk continuity of operations to test potential changes to security measures. In experimental environments, research labs can assess the effectiveness of security measures and potential damage from an attack without risk to the nation's infrastructure. Exploiting this environment, the labs can provide insight into the impact of successful attacks on both the targeted system and the entire infrastructure. Such information is especially important to first responders who must anticipate cascading effects from an attack. In addition, by better understanding possible effects of successful attacks on power generation and distribution, experimental data can support the case for cyber security investments at operator facilities.

State and local governments are the final group of stakeholders. Most local government organizations do not have cyber security experts, nor do they participate in regular collaboration on cyber security issues. However, they are ultimately responsible for physical response and mitigation actions in any location where a cyber intrusion leads to physical damage and a threat to the local population. Therefore, local governmental organizations require information of pending and successful attacks to plan and execute mitigation actions in their local area.

As demonstrated in this section, there are many stakeholders with diverse responsibilities and agendas related to sharing cyber security information. An appreciation for their motivations to interact with each other is important to understanding any potential collaboration and information-sharing framework for cyber security. The next section will address the existing institutions that guide reporting and information dissemination between the stakeholders identified above. As I will show, not all stakeholders are formally tasked to share information, but all participate in information exchange in some manner.

7.3. **Existing Guidelines and Standards for Cyber Security**. According to the National SCADA Test Bed (NSTB) (2005), the first set of cyber security standards, designed specifically for the electric power sector, was created in 2001. Established by NERC, this first set was intended to be preliminary and therefore did not contain significant detail (NSTB 2005). Until 2001, the only source of standards from which operators could develop their cyber security measures was ISO 17799. ISO 17799 is a general cyber security standard designed to help implementers establish all components of a cyber security program. ISO 17799 has now been replaced by ISO 27002. Currently, there are no less than five sources for cyber security guidelines and standards applicable to critical infrastructure control systems to include those in the electric power sector (NSTB 2005). However, only three of these sources contain guidelines for collaborating and sharing cyber security information; the energy sector-specific as input to the NIPP, the NERC Critical Infrastructure Protection Standards, and Industrial Control Systems

Joint Working Group agreements. This section will review these three sources to create a baseline for the expected level of cyber security information-sharing in the electric power sector.

7.3.1. **Energy Sector-Specific Plan.** According to the energy sector-specific plan, the sector's input to the National Infrastructure Protection Plan, there is an imperative to share information across the sector (DOE 2007). With regard to information- sharing the stated goal is to, "Establish robust situational awareness within the Energy Sector through timely, reliable, and secure information exchange amongst trusted public and private sector security partners (DOE 2007, 39)." Proper safeguards on protection of proprietary information are highlighted as the key to reliable and secure information exchange. The collaboration network participants and procedures must be trusted by the private sector actors so they are confident that information they provide will not generate liability costs for them (DOE 2007). Likewise, federal government agencies must be confident the private sector will safeguard information provided on security threats in order to protect sources of the intelligence information. However, the sector-specific plan does not direct any specific actions to protect the information shared in both directions. It simply identifies that the NERC-operated ES-ISAC "gathers, disseminates, and interprets security-related information." The plan does not otherwise detail specific procedures for how the information should be reported or safeguarded. Further details on reporting (but not safeguarding) are left for the current NERC standards.

7.3.2. **NERC CIP Standards**. The current NERC 1300 series of cyber security standards has replaced the 1200 series "urgent" standards drafted in 2001. Within the 1300 series for critical infrastructure protection (CIP) cyber security, one set of guidelines, CIP 008, pertains specifically to developing an incident response and reporting plan (NERC 2006a). According to CIP 008, electric power operators are required to characterize and classify events that would be reportable based on self-determined criteria. The operators are then required to develop a process for reporting the cyber security incident to the ES-ISAC and follow the process for all reportable incidents (NERC 2006a). The asset operators are not required by this standard to report the incident to any other public or private organizations. The only exception is the requirement to submit a DOE 417 if the event results in an electric power reliability concern. In addition, these requirements only pertain to those organizations that have also self-identified as having critical cyber assets that require safeguarding according to the CIP standards (NERC 2006b). Absent a more encompassing set of standards to facilitate information-sharing between a larger collection of stakeholders, it is not surprising that the ESCSWG determined in their 2008 annual report that insufficient progress has been made in this area.

7.3.3. **Industrial Control Systems Joint Working Group**. More recently, the DHS office responsible for control systems cyber security, the Control Systems Security Program, formed the Industrial Control Systems Joint Working Group to address several issue areas such as research and development, international cooperation, and work force development (US-CERT 2009a). The issue of information-sharing is one area for which they have dedicated a sub-group. This sub-group is chartered to study and recommend improvements to several components of information-sharing and information handling within and amongst all CI sectors. One specific objective from their charter is to "Create incident reporting and handling guidelines in order to assist owners/operators with responding to incidents (ICSJWG 2009, 3)." The group has given itself less than one year to "document current information sharing mechanisms" and "develop a clear set of report and incident handling guidelines (ICSJWG 2009, 4)." As with previous measures, the main focus of the group's effort seems to be on the private sector's procedures. Recently, the information sharing subgroup developed a procedure to employ a restricted access web portal to share information between operators and ICS-CERT (DHS 2010b). Although this group's charter acknowledges issues with controlling proprietary information in government databases, there seems to be no publicly available guidance on information-sharing procedures between other actors such as vendors, research labs, and government agencies beyond DHS. In addition, this supports all CI sectors that rely on industrial control systems. None of the measures being developed by this working group are specific to electric power.

7.3.4. **Assessment of Information-Sharing Measures.** As the discussion to this point has highlighted, there are many potential gains from collaborating. Several government organizations, at all levels, play important roles protecting critical infrastructure from and responding to cyber attacks. Since federal and local emergency management responders do not have independently derived situational awareness on the status of cyber systems within the electric power sector, they rely on information from the asset operators to improve their ability to act quickly and effectively. In addition, better information on potential threats and best practices in the hands of asset operators can greatly improve their risk management procedures and support the business case to invest in security (DOE 2009).

But if everyone would clearly benefit from improved collaboration, why are there so few guidelines for information-sharing procedures across the sector, and why have recent reports highlighted continued problems in this area? Most likely, development of and compliance with information-sharing rules suffers from the same challenges that Ostrom (1990) and Olson (1971b) have articulated in their works on collective action. Even though all would benefit from collaboration, there is a strong incentive to free-ride on others' contributions when not otherwise compelled to contribute. In fact, even if the collective made the rules themselves, one can expect an even larger disincentive to comply when compliance cannot be easily monitored (Schelling 2006). In addition, there are so many stakeholders, especially those within the public sector, that private sector actors may be unclear both whom they should provide information to and what benefit they will receive should they provide it (Prieto 2006). The benefits must be made very tangible to the private sector participants, given that any disclosure of information regarding their state of security is a potential liability. Not only must the benefits be tangible, the benefits must be appropriable to individual actors or the incentive to free-ride on others' contributions will persist. Therefore, research needs to explore these collaboration problems. As with any interaction, the interaction space, or network, is an important component of the research problem. Since an extensive literature review was presented in Part I, only select works on inter-organizational network theories that support this research will be presented next.

7.4. **Inter-Organizational Collaboration from a Network Perspective.**

As stated by Ostrom (1990), how a problem is framed "affects which questions are asked and what one looks for in conducting empirical inquiries (pg 46)." I begin this section with a short justification for, and discussion of, applicable network theory. This particular theoretical approach will then be applied to the electric power sector to test two hypotheses.

To begin, we need a useful definition of a network as it pertains to the actors involved in critical infrastructure protection. In this research I will employ the definition of a network form of organization taken from Podolny and Page (1998): “any collection of actors (N ≥ 2) that pursues repeated, enduring exchange relations with one another and, at the same time, lack a legitimate organizational authority to arbitrate and resolve disputes that may arise during the exchange.” The network structure exists in between contractual relationships and formal hierarchies such as a firm (Podolny and Page 1998). In such an arrangement, the participants rely on each other, yet cannot compel compliance to any agreed upon direction (O'Toole 1997). Therefore, instead of contract specifications or employment relations, the participants in a network, either individual or organizational rely on a norm of reciprocity to govern their relationship (Powell 2003). As I will attempt to demonstrate in Chapter 9, this form of working arrangement is an accurate depiction of the environment in which the electric power sector stakeholders interact on cyber security. Since the asset operators are predominantly private, they are clearly not under the hierarchical control of any federal agencies. Also, there are no requirements to share cyber security-related information with the exception of two legally mandated regulations. The first mandatory reporting requirement is the DOE requirement to report electric emergency incidents and disturbances in the United States according to the Federal Energy Administration Act of 1974. According to the instructions on the DOE Form 417, this includes actual or suspected cyber or communications attacks that could impact electric power systems. The other mandatory requirement is the NERC CIP-008 requirement to report all "reportable Cyber Security Incidents."[48] However, it is generally expected that anything that would be reported to DOE via the DOE-417 would be reported to NERC, as well as any other incident that the operator determined was significant (NERC 2008). Beyond these two reporting requirements, there are no codified information-sharing links between stakeholders in the electric power sector. In fact, these two reports create unidirectional flows toward the regulators. There is no requirement for the recipients to fuze information they receive and then share reports with other stakeholders. There is only the general responsibility in HSPD 7 for the sector-specific agencies to "protect" and "secure" their sectors with the assumption this includes providing security information to private sector operators as appropriate. In other words, there is no explicit norm of reciprocity. However, if effective procedures for sharing information between all stakeholders can be emplaced, it is possible that a norm of reciprocity can be

[48] There is no further specificity regarding the definition of "reportable."

established that effectively makes interaction within the network, beyond the two mandatory reporting requirements, a form of consensual contract.

According to one researcher, network forms of organization have become prevalent in public administration for at least three reasons (O'Toole 1997). First, more complex public goods problems require broader coordination of effort across government agencies and with the private actors (O'Toole 1997). Non-traditional security threats, such as those in cyberspace, provide excellent examples of challenges requiring an inter-agency response. As I argued in Chapter 2, the US Defense Department is not well suited to defend the nation against threats through cyberspace. These threats are not countered with military hardware and troop formations that the DOD brings to national security challenges. DHS is equally challenged since it’s primary expertise, and focus, is dealing with physical threats to citizens and property from actors within the US or at the borders. Likewise, DOE is primarily concerned with reliable energy delivery and with mitigating the impact of accidents or natural disasters. Therefore, any effective response to the threat from cyberspace will require the close coordination of several federal agencies partnered with private sector stakeholders. Secondly, efforts to reduce the expansion of government have made network mechanisms for public service delivery and management more attractive (O'Toole 1997). The potential costs of maintaining staffs of cyber security experts for each industry sector would be extensive. Third, political imperatives may drive networking "beyond what might be necessitated by policy objectives (pg 47)." In order to secure wide-spread support for cyber security programs, public administrators must submit to coordinating their efforts with a host of organizations that have equities but may not be able to contribute effectively to solving the cyber security problem. Ensuring the commitment of the critical participants may involve collaboration with many who are not critical to the immediate solution, but are otherwise in influential positions regarding US national cyber security policy. Understanding and coping with this imperative is an additional challenge confronting those leading the charge.

Having argued that networking is an important component of this public policy issue, I will apply the theory to frame the previous stakeholder analysis. This preliminary network model will for the basis of later research. Figure 14 provides a pre-research representation of the electric power sector from a simple network perspective. Ten nodes are depicted in this network. To reduce the network to ten stakeholders and make the network representation tractable, an important convention is employed. The stakeholders that are groups of actors are depicted as a single node. In the case of asset operators, for example, over 2,000 actors are grouped into one node. For the purpose of this work, the similarity of their interactions and motivation to interact should be sufficiently similar as to allow them to be represented as a unitary component. A similar convention is used for the research laboratories, component vendors, and the intelligence community.

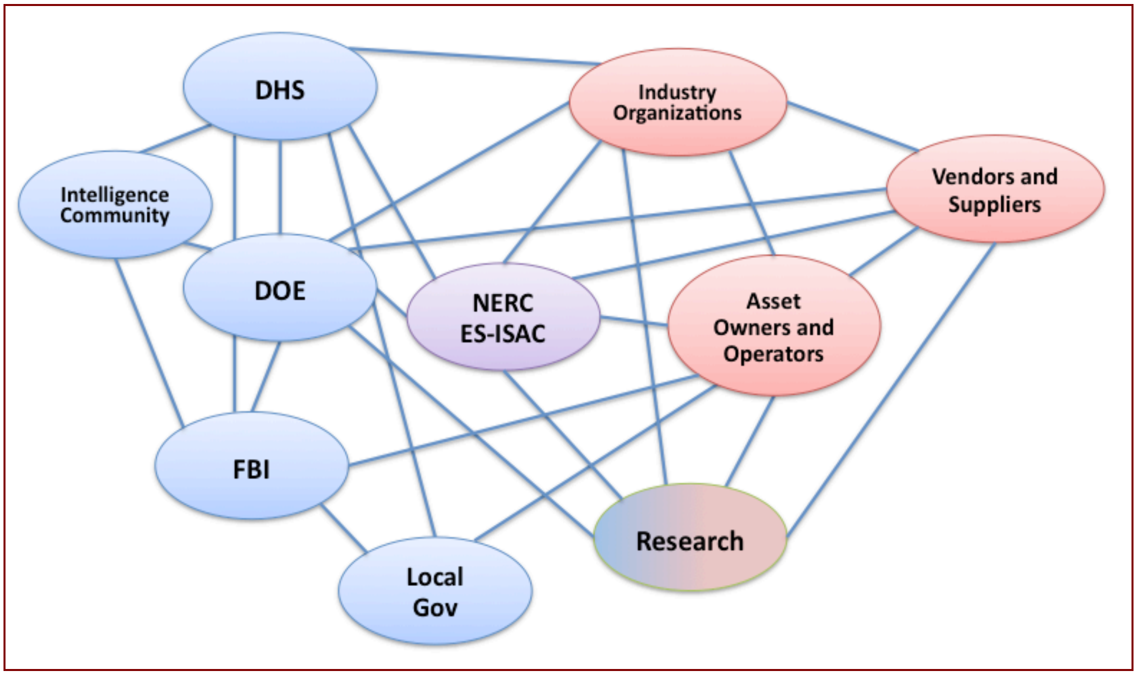

Figure 14: Electric power sector cyber security network: Pre-research perspective.

The links between the actors signify only that the actors are expected to have some level of interaction based on initial document surveys. The links are not valued in that they only depict the expected existence of communication flow, not the expected amount of information flow. In addition, the links are not directed in that there is no depiction of the direction of information flow between nodes. Ideally, information of some significance would flow in both directions along all links. As I will demonstrate in Chapter 8, this depiction most likely does not represent reality, or the perception thereof, amongst the stakeholders. At any given time, one or more of the links between the stakeholders are not functioning effectively. This situation could arise for a variety of reasons such as limited knowledge regarding whom to contact, change-over of personnel, lack of trust, and unfamiliarity with who would need what information.

This rudimentary network structures represent a growing number of relationships between private and public organizations but it also provides a point of departure for analyzing the actual communication flows between the stakeholders. Several authors have demonstrated that networks are valuable tools to understand the flow of information and the way relationships between actors are grown and improved over time. As stated, improving the information-sharing network is an important goal for DHS and DOE. In the next section, I consider the theories of two researchers that support this view, Ronald Burt and Mark Granovetter.

7.5. **Social Interaction within the Cyber Security Network**. Burt, a sociologist at the University of Chicago, is a leading researcher in the field of social network analysis. Three concepts that he employs extensively in his work are; network closure, structural holes, and brokerage. Network closure pertains to how well connected the actors in a network are. According to Burt (2005), a network with many links between all the actors would exhibit substantial closure. This phenomenon is most significant when examining sub-networks within a larger population. When two sub-nets within the population are not well connected by links from one sub-network to another, structural holes are said to exist in the network (Burt 2005). Those actors that do connect the sub-networks, by having links between both collections of actors, are considered to play the role of a "broker" between the two sub-networks (Burt 2005). Brokerage becomes important for phenomenon such as information diffusion and innovation. According to Burt (2005), the broker builds social capital in the collections of actors that they link by creating the information diffusion and innovation bridge between them. In other words, the third-party ties through the brokers facilitate greater trust-building between key actors, such as asset operators and DOE, to increase closure in the network. The increased closure both improves the amount and speed of information-sharing. Both are necessary for effective response to cyber security incidents.

Burt's concepts could be applied to the electric power sector network in Figure 14. For example, a worst-case scenario would depict the network with much fewer actual ties between actors. Such a case would represent a situation where there are only ties between the private sector actors (red nodes) who trust each other to safeguard proprietary, business-related information, because the asset operators and vendors have business contracts with each other that help create trust between the parties. Similarly, there would be a group of actors that are closely tied within the government (blue nodes) who have the appropriate clearances to safeguard information of a national security nature. In the middle would be the ES-ISAC, and potentially joint research centers, who serve to create a link between the two closed networks. Employing concepts from Burt (2005), the ES-ISAC and research centers could act as brokers playing an important role linking the two sub-nets. Their brokerage would allow the flow of cyber security information between the two sub-nets.

Other researchers have focused more on the links between the actors than on the actors' roles. Granovetter, a sociologist at Stanford University, is perhaps best know for his seminal article titled, "*The Strength of Weak Ties*" from 1973. His social networking theory focused on the weak ties between two closely knit networks of friends (strong ties). According to Granovetter (1983), "The weak tie between Ego (an arbitrary individual) and his acquaintance, therefore, becomes not merely a trivial acquaintance tie but rather a crucial bridge between the two densely knit clumps of close friends (pg. 202)." This theory would suggest that it is effective to link together groups even if the ties that bind the two groups are not as strong as desired. In other words, we would still expect important information to flow between groups with stronger internal ties. In fact, the weak tie may reduce possible dissonance between the groups. The groups being connected may have different value systems and motivations. This difference impedes the creation of full trust between the cliques. However, the weak tie would not threaten the internal cohesion in any sub-net and may therefore encourage the flow of some information (hopefully, information that does flow would be significant to improving cyber security).

Granovetter's network concepts can again be applied to the electric power sector network in Figure 14. Another potential network scenario would maintain the strong ties identified in the previous example, but introduce several weak ties between more actors on the left and right sides of the network. Such a representation would acknowledge the influence of working groups, such as the ICSJWG, and other opportunities for the actors across the sector to engage and form ties. The ties may not be equally strong as within the sub-nets, but the continual interaction generates some level of communication and collaboration across a broader space. This example would allow for a Granovetter-type "strong tie/weak tie" analysis. In other words, there would be a potential for a greater chance of important information to "cross the divide" between the public and private sectors amongst actors with weak ties. The existence of weak ties would allow for sufficient integration, and support a division of labor between the sub-networks (Granovetter 1983). The public sector could focus on the threat and mitigation of attacks while the private sector could focus on the "front-line" defenses. The prevalence of weak ties could also create the potential for people to move between organizations and further improve information flow and trust (Granovetter 1983). Unfortunately, few researchers have tested these theories in realistic settings.[49]

Whether employing concepts from Burt and Ganovetter, an important goal would be to foster the growth and collaboration in the network such that it is strong enough to support the rapid flow of critical information and endure in a crisis. In other words, the role of brokers can be encourage to develop more weak ties between sub-nets of more strongly linked stakeholders. However, a critical, yet undefined, number of actors contributing relevant information must contribute to creation of this good. If an insufficient number of members are in the group, or those in the group do not actively participate by sharing relevant information, there is not enough of a contribution to produce a good that is value-added. As, for example, when a small community cannot collect enough funds to build a pool, there is not enough information being provided to ES-ISAC and the DHS cyber security centers for them to collate, fuse, and re-distribute a valuable product.[50] This concept is similar to the idea of the tipping point regarding

[49] The proponent himself lamented the fact that few of his theoretical assertions on the strength of weak ties have been empirically validated (Granovetter 1983).

[50] If this were the case of a club good, defined by James Buchanan (1965) to be mostly non-rivalorous but excludable (e.g. a community pool), as long as enough members are induced to contribute to a “value-possible” level, there would be a potential to generate a sustaining

cyber security investment introduced in Part II. In both cases, a critical coalition could encourage participation by others. However, if the others are allowed to free-ride by receiving information without having to contribute, there will be a strong incentive to continue to do so. In the case of cyber security information-sharing, DHS cannot easily make their products club goods as they are required to provide support to all who desire it. They cannot limit their support only to those who contribute valuable information to their cyber security centers.

In this chapter, I introduced the information-sharing aspect of national cyber security as it pertains to the electric power sector. I identified the ten important stakeholders and described a theoretical network linking the stakeholders. I also identified the limited, formal information-sharing requirements between a small set of actors and network theory that informs an analysis of the interactions throughout the network. Both Burt and Granovetter have developed networking concepts that can be applied to an analysis of cyber security collaboration between the stakeholders in this sector. The limited amount of formal information-sharing will form a point of departure for my research in Part III. In the next chapter, I will present the research methodology to test theories raised both here and in Part I. These

information-sharing network. This outcome would be possible because, once firms start receiving a value-added product, they will be further encouraged to become members of the club.

theories will be employed to explore the actual composition of and motivations to contribute to the cyber security information-sharing network.

8 Methodology

8.1. **Research Question and Hypotheses.** The purpose of Chapter 8 is to indentify the primary research question and hypotheses for Part III then present the methodology employed to explore the stated hypothesis and alternates. In Chapters 1 and 2, I identified the critical components of private sector contributions to national cyber security. Private sector actors must increase their investments in cyber security measures and contribute to information-sharing networks that improve security postures and respond quickly to security incidents. In Part II, I presented results of research regarding the coordination and implementation of security investments in the face of substantial disincentives to invest cyber security measures. In Chapter 7, I showed there are also barriers and disincentives to share cyber security related information between private sector actors and the federal government cyber security agencies. The goal of Part III is to increase our understanding of the motivations to share important cyber security information in spite of these barriers. Research Question 2 contains the specific goal.

Research Question 2:

How can public-private information-sharing networks be improved to the level that the information-sharing becomes a value proposition in both directions?

The first step in exploring this question is to verify an important assumption contained therein. In Chapter 7, I presented a theoretical network of the relevant stakeholders in the electric power sector based on their general relationships to each other. However, this visualization tool is merely that. It should not be assumed that information actually flows between any of the depicted linkages in this CI sector just because the stakeholders were identified in the National Infrastructure Protection Plan and other documents that identify the need for partnering. Therefore, the first task is to determine whether any form information-sharing network exists between these stakeholders. Hypothesis 2A addresses this task.

Hypothesis 2A: Stakeholders in the electric power critical infrastructure sector participate in an information-sharing network to exchange information relevant to cyber security.

It is important to confirm Hypothesis 2A before proceeding so that I do not make faulty assumptions regarding the existing of any type of information-sharing mechanisms. In Chapter 7, I explained the roles of ten stakeholder communities in the electric power sector. All stakeholders have either self-identified or have been identified in federal government documents as playing a role in cyber security for the sector. Some have explicit reporting requirements and others have informal ties with the other stakeholders. Using the network definition presented in section 7.4, I will look for a collection of actors that interaction without formal requirements to do so and their paths for information exchange. Whether formal or informal, the paths used to exchange information create a network that will become important during times of cyber security crises. If no network exists, then new paths for information-sharing must be created during crises and the time required to building trusting links will severely hamper preparation and response efforts. Therefore, this hypothesis does not make any distinction regarding whether the network is formal or informal. Also, there does not need to be an identifiable network between all ten stakeholders, but some communication path must exist between private sector operators of electric power generation, transmission, and distribution and the federal government agencies responsible for cyber security. The path may be e-mail distributions, formal reporting, periodic meetings, or frequent review of information available on web-based portals. To satisfy the established network definition, information should flow in both directions on identified links so that a norm of reciprocity can be expected. Once a network has been identified, the research can proceed to the primary hypothesis regarding motivations to share cyber security information.

The National Infrastructure Protection Plan highlights the roles the private sector played in developing infrastructure protection measures (DHS 2006). Since the private sector has been relied upon heavily to craft and to implement the national cyber security regime, the theory of empowerment should be useful for this research. Empowerment studies have spanned from the individual level to the team level and higher levels as well as across multiple levels. Spreitzer's (1995) research on empowerment focused on the perceptions of those allegedly being empowered. Her studies sought evidence of a perception of empowerment based on four components: meaning - belief that the work is of value; competence - belief that the worker is capable to perform the specified actions; self-determination - perception of choice in actions; and impact - degree to which outcome is effected (pg 1443). The concept of "self-determination" and "impact" relate directly to assertions by DHS and the authors of the National Infrastructure Protection Plan (NIPP). For example, Appendix 1A of the NIPP which details cyber security programs, states, "The private sector is *encouraged* to implement the following recommendations...(pg 111)." The recommendations include: *participating* in sector-wide programs to share information on cyber security, *participating* in industry-wide information-sharing and best practice dissemination, and *promoting* industry guidelines for cyber security (DHS 2006). Several components of the plan also highlight the role that industry trade associations played to develop the plan. In other words, the impact (degree to which outcome is effected) of the private sector efforts was the development of a plan for national infrastructure protection. The significance of this act is that DHS is expecting to motivate private sector participation in national security, and that participation will soon lead to sharing of relevant information that can be assimilated, analyzed, and turned into value-added products to improve cyber and other security efforts. The first step in this process is ensuring the private sector actively participates and contributes relevant information. Applying this reasoning to the electric power sector leads to the following hypothesis.

Hypothesis 2B: Private firms in the electric power sector will contribute to the collaborative, information-sharing network because they and their industry representatives contributed to the development of the information-sharing protocols.

This hypothesis applies specifically to the electric power sector because the relevant aspects of the information-sharing network for national cyber security are unique to each sector.[51] For the purpose of this research, "contribute to" means to provide information into the network.[52] This information can be exchanged via e-mails, formal reporting channels, or

[51] The theories being employed in this work may be generalized, but the results from analyzing this specific hypothesis should not be applied directly to all sectors regardless the findings.

[52] It would be more appropriate to state that such information should be valuable information that could help fusion centers develop a clearer understanding of the threat vectors, however this criteria would be highly subjective and cannot be directly measured.

recurring, face-to-face meetings. Though the focus of this hypothesis is the commercial operators, it acknowledges the potential influence of representative agents. Industry representatives include employees from other private firms, public-private partnership organizations (e.g. sector coordinating council), and the ES-ISAC. Information-sharing protocols are those that are found in the National Infrastructure Protection Plan, the NERC CIP standards, and procedures created by the Industrial Control Systems Joint Working Group.

To strengthen the validity of this hypothesis, the research will also explore the potential for several alternate hypotheses that may show different motivations to participate:

Hypothesis 2B (rival 1): Firms in the electric power sector will contribute to the collaborative, information-sharing network because they desire to avoid additional government regulations.

Several studies of self-regulation activities have addressed the motivation to avoid governmental intervention in their industry (see, for example Gupta and Lad (1983b)). Though their results were inconclusive, King and Lenox (2000) sought to find evidence that self-regulation in the chemical sector would lead to an improvement in corporate behavior (mostly in the area of pollution) when the companies enact measures to avoid governmental regulations. Whether the actions are measurably effective, the motivation to enact them to avoid further regulation has been shown to be potentially strong in previous studies and provides a potential alternative hypothesis for this study.

Hypothesis 2B (rival 2): Firms in the electric power sector will contribute to the collaborative, information-sharing network because linkage to federal government agencies was fostered by third-party actors that the firms trust.

According to social networking theorist Burt (2005), strong and positive third-party ties between two actors invoke greater trust between the two actors and add closure to the interaction network. This action lowers the risk for either person to trust the other and potentially improves the flow of communication. Given that several actors intervene between, and with, the private firms and the federal government in the information-sharing network, these third-party actors may be responsible for strengthening the important links and motivating collaboration.

8.2. **The Electric Sector Case Study.** In Part III, I employ a case study approach to explore the hypotheses associated with the information-sharing dimension of the cyber security problem. As identified in the hypotheses above, the focus will fall on several private companies, and power management administrations, in the electric power sector that have collaborated with DHS and DOE on cyber security.

The case study will follow a single study, embedded design, consisting of interviews, document reviews related to sector-specific cyber security measures, and observation at industry working group sessions. A single case study, embedded design, method is appropriate for several reasons. According to Yin (2003), a case study is an empirical inquiry that "investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident (pg 8)." Accordingly, national cyber security, and the development of information-sharing protocols in the electric power sector are contemporary events (Hare 2009). Second, case studies allow the researcher to continually improve the interview instruments before the final interviews based on observations and document reviews (Yin 2003). As this case study will show, each stakeholder has a unique cyber security organizational structure. Through interviews, I could assess and adapt study questions to each respondent's unique structure. Third, it is a favorable method to use when the researcher wants to include or account for contextual factors and when the researcher cannot control behavioral events such as one attempts to do in an experiment (Yin, 2003). The national cyber security information-sharing networks consist of public-private partnerships that are specific to each sector of critical infrastructure. The complex stakeholder relationships in the electric power sector require that the analysis of these relationships be as focused as possible. Fourth, the researcher can consider the unit of analysis and its connections to other actors as a whole entity, reducing the need for assumptions (Ragin, 1987).

8.2.1. **Units of Analysis**. Since the issue being studied in Hypothesis 2A and B are different, they require different units of analysis. Each is presented in this section.

8.2.1.1. **Hypothesis 2A Units of Analysis**. To identify the existence and structure of the information-sharing network, the units of analysis should include as many stakeholders from the pre-research network as possible. Though short of this goal, nine respondents representing DHS, DOE, NERC, vendors, private sector operators, and DOE enterprise operators are all included in the sample for this study. However, this sample composition did allow for some insight into the actions of other stakeholders with which the respondents interacted. Considering multiple perspectives also validates the linkage and helps the researcher to understand if the flow of information goes in both or either directions. By including multiple perspectives of each interaction, I am also able to better tailor the interview instrument for assessing the second hypothesis.

8.2.1.2. **Hypothesis 2B Units of Analysis**. The units of analysis for hypothesis 2B, the motivation to share cyber security information, consist of four private sector firms that generate and/or transmit electricity. The firms were selected based on discussions with an electricity sector security expert at the North American Electric Reliability Council (NERC) and interaction with potential respondents at industry forums. The sample was not randomly chosen, but consists of major corporations that are actively involved in developing the cyber security measures for their organization and the information-sharing regime for the nation. Specific interview respondents were either personnel from the firms' office responsible for developing and implementing cyber security measures for control systems, or the office that ensured compliance with those security guidelines. Though there is a potential for principal/agent problems when only interviewing few, non-leadership individuals at each firm, the small size of the responsible offices, and their access to senior decision makers, should compensate for such error.

8.2.2. **Case Study Protocol**.[53] Initial research planning occurred at Government First Responder (GFIRST) conference in 2007. GFIRST is a group of cyber security experts responsible for securing government IT systems (US-CERT 2007). By attending GFIRST, I was able to identify many relevant government documents necessary to prepare for the interviews. These publications included the sector-specific plan for the energy sector, as called for in the NIPP, and documents related to the industrial control systems working group under the Critical Infrastructure Partnership Advisory Council (e.g., minutes, charters, and newsletters). Through observation and participation in electric power sector cyber security working

[53] Substantial portions of the next three sections were taken from previous, preliminary research work and my article published in the *Journal for Homeland Security and Emergency Management* (Hare 2009). The information has been updated based on the details of the current research.

groups, the interview questions were tailored to address the specific issues surrounding Hypothesis 2A and 2B. The next data-gathering stage consisted of interviews with DOE cyber security officials as well as a member of the Electricity Sector Information Sharing and Analysis Center at NERC. Participation at a DHS-organized conference for industrial control system cyber security allowed me to identify potential respondents and conduct interviews with several of them. The final stage consisted of interviews with participating private sector firms using a combined, open-ended and direct question interview instrument. The interviews were conducted both in person and via phone. In each case, I provided the respondents with the opportunity to review my transcribed notes and correct errors or provide additional details.

8.2.3. **Data Analysis**. The primary source of evidence to assess the main and rival hypotheses comes from answers to interview questions. Several questions focus on the respondents' perceptions as to what information they generate regarding their cyber security posture and with whom they share the information. Additionally, I ask each organization about sources they rely on for cyber security threats and vulnerabilities. This information helps us to understand if and how information flows in both directions on a dyad.

By attending working groups and conference, I observe what information is being directly provided at the events and learn of concerns that stakeholders have regarding sharing information with each other. The interview instruments contain several questions that address private firms' contributions to the national cyber security regime and why they would share cyber defense-related information with the federal government. The core questions are asked in different ways and to several stakeholder communities to gain greater insight into the issue. For example, if the respondents from the firms answer that they are motivated to contribute as a result of theirs or their trade association's participation in development of the regimen, it suggests that empowerment did play a role for their firm based on the components of empowerment identified by Spreitzer. However, if the respondents do not acknowledge a familiarity with the process used to develop the applicable security measures, they cannot relate to the contributions of their agent. Therefore, empowerment should not be considered a significant factor.

Observation of, and participation in, industry working group sessions also provides insight on how the private sector contributes to the development of security measures and standards. While active participation at these events does not provide evidence of causal linkages, it can demonstrate actions supportive of empowerment theory (observed behavior of actively constructing the information-sharing procedures) and a desire to collaborate through the working group.

8.2.4. **Validity Measures.** Construct validity is ensured through three measures. First, the study uses multiple sources of evidence to converge on the possible hypotheses. The sources include three different sets of interviews from three different perspectives- federal government, “betweener” (the NERC), and private firms, as well as observation during working group events. The second measure will be the creation of a chain of evidence through the construction of a research database that will be available to other researchers to verify content and review evidence. However, for confidentiality resources, several private sector respondents asked that their identity be masked. Lastly, the DOE cyber security office was asked to review the findings. A review session was conduct with DOE in June, 2010. DOE did not identify any significant issues with or different interpretations of the findings. Internal and external validity of findings regarding Hypothesis 2B is ensured by matching results to existing theories employed to develop the main and potential rival hypotheses.

9 Analysis and Findings

9.1. **Introduction.** In Chapter 9, I will discuss the findings of my research regarding Hypotheses 2A and 2B. First, I develop a revised model of the information-sharing network in the electric power sector to support Hypothesis 2A. The revised network model is based on document reviews, observations at DHS and DOE-led events, and interviews with nine stakeholders in the electric power sector. With the network more accurately modeled, I turn to the primary goal of the research for Part III, improving our understanding of the motivations for sharing cyber security information in this CI sector. All information-sharing is of potential value to the federal government agencies responsible for securing the nation in cyberspace. In order for this information-sharing effort to be of value to the private sector participants as well, the assembled information must be turned into knowledge that will improve their cyber security postures. At a minimum, the benefits of the information the private sector receives should outweigh the actual costs of providing the information. Such costs are realized through time spent completing forms, reviewing compliance measures, and briefing leaders on interaction with regulators. For this dissertation, I study one primary and two alternative hypotheses to explain how private sector participants are motivated to contribute cyber security information beyond the minimum amount required to comply with regulations. According to my observations from interviews, the DHS view that empowerment motivates cooperation should be adjusted to account for the role that trust plays in the dynamic between private industry and the federal government. The study interviewees acknowledged being participants in the processes to develop information-sharing procedures and felt that their participation was important. However, they did not view themselves as having been empowered by DHS in the way that previous researchers would define the concept. Consideration of the rival hypotheses supported this finding. Respondents did feel that third-party actors created stronger connections between the private sector and public sector by helping to bring all the important stakeholders together more often. According to respondents, the increased interactions facilitated by these third parties improved trust between the stakeholders. Increased trust leads to stronger communication paths.

In the next section, I will present a refined model of the information-sharing network as revised through observations and interviews. This model is helpful to place the responses related to Hypothesis 2B in a conceptual framework.

9.2. **Analysis of Hypothesis 2A**. The previous conceptual network developed from a preliminary document review was not intended to depict the industry network for sharing cyber security information. The depiction was only intended to serve as a baseline by showing general relationships between stakeholders. While the document review helped develop a starting point, it was necessary to include observation at CI cyber security events and to conduct interviews with key stakeholders in order to develop a greater understanding of cyber security information flows between stakeholders.

9.2.1. **Observations and Interviews**. By attending a DOE-led cyber security workshop and a DHS-led control system security event, I gained several insights regarding existing information-sharing links and stakeholder concerns with sharing data. First, of the six sub-working groups within the Industrial Control System Joint Working Group, the information-sharing sub-group has one of the lowest levels of industry participation.[54] This observation would suggest limited interest within the private sector for sharing information. However, during the general meeting of the full working group, the private sector participants asked a substantial number of questions of ICS CERT personnel regarding information-sharing procedures

[54] The other five sub-groups are; International, Vendors, Work Force, Research and Development, and Roadmap.

and safeguards. During both the DHS and DOE events, there was extensive discussion regarding ways to obtain classified and unclassified threat data from federal agencies. Clearly there is a desire to receive this type of information to support cyber security measures at operator facilities. Discussions regarding the establishment of a web portal at DHS for control system security information, and further discussions of the initiative at the DOE-led event, highlight a desire to share information in both directions. On the other hand, the cyber security personnel at both events expressed frustration with providing information and a fear of retribution from compliance organizations when incriminating information is provided. Lastly, discussions regarding the publication of a joint analytic product at the DOE-led security workshop provided positive evidence that NERC, DOE, the FBI, and DHS are all collaborating on cyber security analysis. This cyber security product has been provided to all electric power operators via a NERC bulletin. According to the ES-ISAC, this information was well received (Roxey 2010). The importance of this exchange of information between NERC, DOE, and the private sector is that it establishes the norm of reciprocity between the public, private, and "in-between" organizations. This norm supports the conclusion that the relationship meets the current definition for a network structure.

Interviews with several stakeholder communities provided further insights into the actual structure of the information-sharing network. Through their answers to interview questions, the respondents provided information about whom they interacted with the most, what type of information they provided to other stakeholders, and what information they received from other sources. To a limited extent, I was able to compare perceptions at each end of links regarding how much interaction occurred between the stakeholders. The interviews also allowed me to gain a better understanding of several barriers that create principal-agent problems within the network. Lastly, attendance at the cyber security events and discussions with interview respondents allowed me to identify stakeholders who were not highlighted in the original network model in Chapter 7. These entities, such as the DOE power management administrations, had been considered sub-entities of the ten stakeholder communities discussed in Chapter 7. Discussions with the nine interviewees led me to conclude that each should be independently identified in the network.

The responses to interview questions presented in Table 1 below provide examples of all three adjustments to the network model. First, a set of interview questions asked the respondents to provide their assessment of the role of various organizations involved in cyber security for the electric power sector. The responses to these questions helped identify whom this sample of stakeholders considered to be central actors in the cyber security network. For example, Private Operator 3 considered the ES-ISAC to be a central actor playing a potentially significant role in disseminating operationally relevant cyber security information. He felt, however, that the ISAC is currently ill equipped to do so. Second, principal-agent and other structural barriers were frequently cited as reducing the effectiveness of the network. For example, the cyber security experts at each organization are considered to be the principals in this network. The cyber security operations staff are the best positioned to know what information to share and how to respond to intelligence they receive. However, because of the concerns of compliance penalties, the agents at commercial electric power companies who actually report information to the NERC are the compliance officers. Unfortunately, compliance officers are more concerned with the chance of penalties and are motivated to provide as little information to the regulatory body as possible to reduce the risk of an audit.[55] Lastly, the interviews led to a greater understanding of the significant stakeholders in the information-sharing network. For example, I had not identified the unique position of the DOE power management administrations (PMA) in the original model. Although they are part of the DOE enterprise, they are more like private sector operators than DOE headquarters regarding their role in the

[55] This barrier appears to be unique to the electric power sector. Other CI sectors do not combine their ISAC with their regulatory agencies.

information-sharing network. However, the PMAs do not interact with the ES-ISAC directly. They only report to a similar organization within the DOE enterprise called the DOE Cyber Incident Response Capability (CIRC). Adding the PMAs and the DOE CIRC to the network means that there are no fewer than three organizations that have information-fusion and analysis roles for the electric power sector; ICS-CERT (DHS), the ES-ISAC (NERC), and DOE CIRC. All three have different restrictions on the information they can pass to each other. The restrictions are designed to protect anonymity and the proprietary nature of information sources.

The relationship between vendors and the other stakeholders must also be highlighted. The vendors have a direct relationship only with their customers but they do get reports from federal agencies when the information has to be made available to everyone in industry. Beyond that, vendors share and receive little information with anyone outside their customer base in the private sector and DOE PMAs.

Table 1: Selected responses informing the information-sharing network structure.

Network Issue	Representative Question	Selected Responses
Identification of Central Actors	From your viewpoint, what is the role of the ES-ISAC?	*Private Operator 3: The ES-ISAC needs to grow. It should be gathering information, analyzing it, and disseminating it to those who need to know. This would reduce the amount of places everyone needs to go to get information.* *It should be gathering information on vulnerabilities from more than industry sources. I'm not sure if that is really happening. They should be working with other sector ISACs. Some vendors are now working with NERC/ES-ISAC disclosing vulnerabilities and providing mitigation recommendations.* *PO3 will send relevant information (not reports on noise) and hopefully the ISAC will utilize it.* *ES-ISAC should also fuse information from US-CERT and provide in products to the sector.*
Principal-Agent Barriers	What disincentives/barriers do you have to sharing cyber security information with other stakeholders?	*Private Operator 2: Sharing information with industry and lessons learned sessions has stopped because they are concerned about fines. Now lawyers have to review all information. Compliance has poisoned the sector's efforts for reliability and security.*
Identification of Stakeholders Communities	From your viewpoint, what is the role of the ES-ISAC?	*Government Operator 2: We have no direct linkage with it since the ES-ISAC only serves private industry. PMAs are required to report incidents to the DOE-CIRC. PMAs are not legally allowed to share directly with ES-ISAC.*

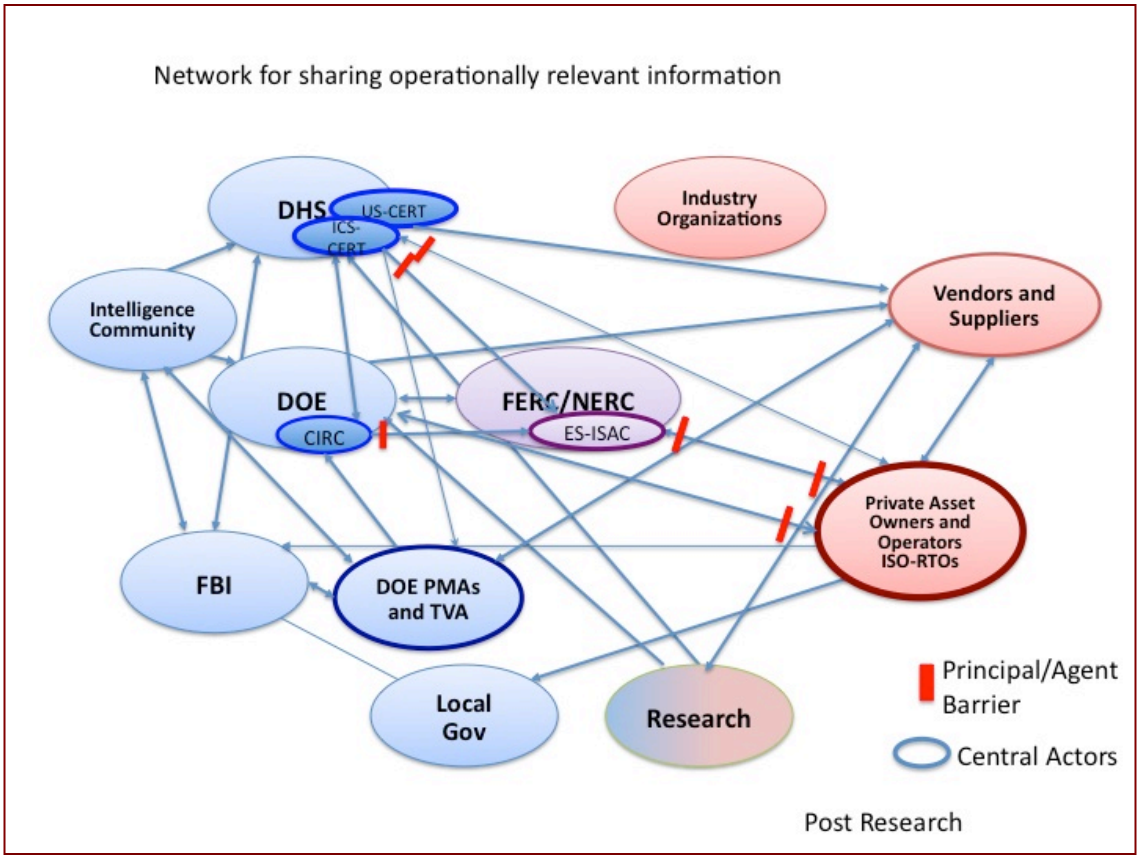

Figure 15: Post-research information-sharing network model.

9.2.2. **Revised Network Model**. As a result of these observations, I now model the sharing of cyber security information in the manner depicted in Figure 15. As one can see, not all the central actors share information with each other and not all stakeholders are broadly connected in the network. For example, electric power operators in the private sector do not tend to share information regularly with operators in the DOE enterprise. It is also apparent that all community stakeholders do not provide information to a common hub to be analyzed and redistributed to the entire sector. Even the three central actors mentioned above do not collaborate to create one cyber security product.

In the revised network diagram, I also depict the existence of institutionalized, principle-agent barriers to sharing information. These barriers act to reduce the significance of the affected link, in that they reduce the amount of information that can be shared across it. There are two categories of barriers depicted in Figure 15. First, the most frequently cited concern from private sector electric power operators about sharing information with NERC is the threat of compliance penalties. The compliance issue creates a barrier in two ways. Because the recipient of the cyber security report is also the compliance organization, any information provided to NERC could create the potential for a compliance inspection. Also, in order for the report itself to be compliant with NERC reporting requirements, more time is spent formatting documentation than conducting productive cyber security actions. As a result of these compliance concerns, every cyber security report from the cyber security team at the operator facility (the principals) must first pass a review by a compliance officer (agent) at each company before the compliance officer shares the information with NERC, FERC, and DOE. Both the fear of an audit and the time expense in reporting act to reduce the amount of useful information that can be provided to government agencies. The barriers resulting from compliance concerns are shown in Figure 15 along the link from private asset operators to the ES-ISAC and to DOE. The other category of barriers identified by interviewees and through working group observations is the requirement to safeguard proprietary information, information "for official use only," and protected critical infrastructure information (PCII).[56] In these cases, there are legal restrictions that keep the fusion centers from sharing reporter-specific details with other recipients who may benefit from them. Once again, information dissemination must be constrained to reduce the risk of disclosing proprietary information, in the case of commercial entities, and "official" information, in the case of reporting by DOE PMAs. Such barriers appear along two links in Figure 15. When the ES-ISAC (agent) provides information it receives from one owner operator (principal) back to the rest of that stakeholder community (also principals), it must anonymize the information to protect data specific to the reporting entity and that others may use to gain a competitive advantage. When DOE CIRC (agent) desires to share data from the DOE enterprise to ES-ISAC, it must also anonymize reporting from PMAs (principals) to protect data that is considered to be "for official use only." Finally, when the ICS-CERT (agent) provides reports based on PCII data to any recipient outside the federal government, it must

[56] "For Official Use Only" is a handling restriction used by the federal government to reduce risk of disclosure of information that could adversely impact the conduct of Federal programs essential to the national interest. PCII is defined under 6 U.S.C. 131(3) (Section 212(3) to refer to information not customarily in the public domain and related to the security of critical infrastructure or protected systems.

also safeguard details specific to the reporting organization (principal). The aggregation of barriers created when these agents attempt to share information on behalf of the principals in this network results in a disturbing observation. Most of the barriers directly impact the ability of the ES-ISAC to receive, analyze, and disseminate operationally relevant cyber security information. The ES-ISAC receives significantly filtered information from both government sources and private sources as the principals act to reduce their liability and other exposures.

This network model can now be analyzed according to the concept of structural holes and the role of brokers discussed in Chapter 7. At this point, it is not clear to this researcher that the ES-ISAC plays a leading role as a broker between the government and private sectors, due to the information-sharing barriers in place. It is also not clear that any other organization is the sole broker. Instead, it appears that all three central actors described previously played a limited brokerage role between the government and private sectors. This observation may not imply a fundamental problem with the network. As long as DOE, DHS, and NERC work together closely, the combination of actors may accomplish the brokerage role necessary to link the important stakeholders.

In spite of the principal-agent barriers and structural holes discussed above, I found several instances of information-sharing between stakeholders in the sector. Though not all actors are linked in Figure 15, the figure shows a network with several important links between the central actors and the electric power sector operators who participated in this research. Since information and data analysis were found to flow in both directions along links between the operators and the brokers, I determined that there is a norm of reciprocity in the network. In terms of Hypothesis 2A, this evidence supports the finding that stakeholders important to the cyber security of the electric power critical infrastructure sector participate in an information-sharing network to exchange relevant, cyber security information. With this conceptual framework established, the next step will be to explore possible motivations for the private sector to contribute to the information-sharing regime.

9.3. **Analysis of Hypothesis 2B.** Personal interviews of electric power sector stakeholders provided the most insights for studying Hypothesis 2B. The interview instruments were based on observations and document reviews, but the subjective nature of this hypothesis required direct engagement with the relevant stakeholders. The most important findings were derived from the interviews with the four private sector operators who have been identified as the units of analysis. These interviews occurred between April and May of 2010. Hypothesis 2B and its rivals will be discussed in order in the following sections.

9.3.1. **Empowerment.** Discussions with interviewees suggest that there was a substantial feeling of self-determination in development of the cyber security regime in the electric power sector. Self-determination is an important component of Spreitzer's theory of empowerment. However, the self-determination that interviewees spoke of appeared to precede the beginning of efforts by DHS to build a national cyber security regime. For example, all respondents felt they had established robust cyber security programs before government prompting to do so.[57] In fact, the interviewees did not think the recent government direction regarding specific cyber security actions and investments would improve their security posture. Also, the companies were proud of their contribution to the development of industry cyber security measures—another important component of the theory of empowerment. However, in all cases, they described contributions to the cyber security regime that were initiated before DHS began to play a role in this area. In other words, these findings suggest that private sector operators felt they were empowered *in spite of* DHS. Table 2 below contains a sample of responses to three empowerment-related questions that support this finding.

The first question in Table 2 pertains to the sole DHS document containing guidance on cyber security information-sharing, the sector-specific

[57] This does not necessarily mean that the programs are effective.

plan under the NIPP. Even though most respondents acknowledged their participation in developing the only official planning documentation, it was not a product in which any respondent demonstrated pride of authorship. In other words, the respondents did not feel the product was valuable. Recognizing this position is important, because the opposite view, a perception of the product being valuable, is an important component of Spreitzer's empowerment theory. When asked about their contributions to information-sharing initiatives in general, all respondents mentioned contributions and initiatives they led themselves. The answers to the second question in Table 2 support this point. None of the respondents mentioned DHS-led, or initiated, projects. Taken together, these responses do not support the hypothesis of empowerment and undermine the idea that the federal government is responsible for empowering the private sector to shape the cyber security information-sharing regime, and that the actions motivated their participation in cyber security. However, all respondents had a common perception that private sectors operators have a significant role in developing standards. In other words, actions designed to empower the private sector may lead to greater motivation to participate, but the motivation did not derive from a sense of empowerment. Instead, the motivation to participate in the network stemmed from the greater level of trust that was built through the working groups and other interactions facilitated by the federal agencies.

Though the results cannot be stated with any level of statistical significance, the responses from the interviewees force us to question the assumption that empowering the private sector to create the cyber security regime will be the direct motivation for private companies to participate in the regime. Electric power sector operators have been concerned about cyber security since well before official institutions began to request their support for formalized information-sharing procedures. Compliance requirements are adversely impacting the relationship, but there are indications that increased trust gained from empowerment efforts can counter-balance this. In the end, the desired effect of increasing information-sharing may be achieved.

Table 2: Sample interview responses related to the theory of empowerment.

Sample Question	Selected Answers
Are you familiar with the contents of the Electric Sector Specific Plan annex to the National Infrastructure Protection Plan?)	*PO1: Yes, we helped write the plan. I sit on the electric sector coordinating council.*
	PO2: Yes, we did provide comments on the plan while it was being drafted. However, the document does not provide much by way of an actual plan. It does not go much further than the step of cataloging what needs to be protected.
	PO3: We have looked at and reviewed the plan, but it is not a key document for PO3.
Did you or your organization play a role in developing the cyber security information sharing procedures for your sector?	*PO1: Yes, it did.*
	PO2: Our organization helped NERC set up the structure for HYDRA. The intent of HYDRA is to setup a community teleconference for immediate triage to focus a NERC alert before it is broadcast. They did a teleconference recently, but the process is still having trouble meeting an effectively short time line. Should get better with practice.
	PO3: Yes, active role. Within ISO/RTO council, there has been a security working group for many years. They shared best practices and information on vulnerabilities well before being told to do so. PO3 was active in the ES-ISAC working group through CIPC.
	PO4: Yes, they did but not sure how much.
Do you think that your organization's contribution motivates you to collaborate more closely with other stakeholders in your sector (e.g. ES-ISAC, DOE, and DHS) regarding cyber security?	*PO1: Yes, it did, but compliance concerns have created significant barriers that keep the collaboration from happening.*
	PO2: Yes, private industry is concerned about change management and is willing to be co-opted. More willing to contribute to the security regime as a result. However, it is easier to get private industry to internalize and self-motivate if they can better understand the "why." In other words, provide them with a clear understanding of the threat.
	PO3: Culture in the ISO/RTOs is to share information. More about learning from each other. At the federal level, there is no real mechanism for sharing information. Information sharing consists mostly of ad hoc meetings. *We have not seen any activity that would warrant submitting a report to CERT. If we saw activity that we felt was of interest then we would communicate it to CERT and ISAC.*
	PO4: Yes, it did help because it allowed you to learn who the other stakeholders are and who to communicate with.

9.3.2. **Regulation Avoidance**. Though several researchers have theorized that a desire to avoid government regulations will motivate self-regulation, the observations made through this research do not provide clear support for that theory. Most interviewees responded that the threat of additional regulation is not impacting their motivation to share information. However, the compliance issues identified earlier seem to create an interaction effect that is difficult to discern. In other words, the interviewees' main concerns are that greater regulation will lead to a greater reporting burden and fewer resources devoted to actually improving security. Table 3 contains evidence to support this finding. For example, Private Operator 3's response to the second question in the table highlights the concern well. On the one hand, Private Operator 3 acknowledges that regulation is necessary, but on the other, he is concerned that the increased compliance burden will reduce resources available for effective cyber security. In addition, none of the respondents to either question in Table 3 stated that increased regulation would reduce their motivation to share important information. In fact, it may be possible that companies would be prepared to take additional steps to secure their systems if it were a cost that all companies would incur. Specifically, they are concerned that the potential security regulations be sufficiently clear to allow for a common understanding of the measures that must be implemented at operator facilities, and not leave them at a competitive disadvantage. Unfortunately, Private Operator 2's response to the second questions suggests that some are not optimistic that any new regulation can be implemented in a way that will improve clarity.

Table 3: Responses to questions related to the threat of additional regulation.

Sample Question	Selected Answers
Are you aware of current proposed legislation? How do you think they will impact information sharing?	*PO1: Yes, but it should not impact information sharing. May create more reach out. NERC has not done well in preparing standards or operating cyber security compliance organization. Current legislation will address some systemic issues, but until the associations are pulled back and their social impact on Agencies, Congress and staffers controlled, we will continue to see confusion in the cyber security theater.*
	PO3: Yes, we are aware, but PO3 does not fully understand them and I do not think legislators understand them. For example, there is apparently a provision where o/o may be directed to "shut down access" to the Internet. But the regulator has no idea what the unintended consequences of that action may be. We do not think the FERC should have more control because FERC does not have many cyber security experts. Too many lawyers directing the standards and compliance measures. NERC and FERC should be segmented. We do not perceive them as currently being separate entities. The current legislation probably won't impact information sharing unless compliance becomes the over-riding emphasis. Reporting efforts need to be anonymized.
	PO4: Yes, and we are very concerned about who will win fight about who will have right to direct what actions are implemented. For example, some legislation suggests imposition of compliance timelines that are dangerous. If measures are not ops checked for a sufficient period before implementation, they may create an even larger risk than non-compliance.

Table 3 (cont.): Responses to questions related to the threat of additional regulation.

Sample Question	Selected Answers
Are you concerned about the possibility of restrictive government regulations in the area of cyber security? If so, how much so and how do you think that would impact your current level of participation in the national cyber security network?	*PO1: We are not concerned about restrictive government regulations, but would welcome clearer guidance. It would make participation better.*
	PO2: Very concerned. There are good people at FERC, but many have no experience with being a part of the industry in a regulatory environment. For example, many auditors have never implemented a security program themselves. They do not understand potential impacts of measures. For example, there have been cases of power being shut down inadvertently upon implementation of security measures. *Organization is very sensitive to over regulation. However more regulation will most likely not impact current level of participation.* *Clear guidance in regulation should not be expected because of the variability of infrastructure and operations.*
	PO3: We are concerned with the possibility they will focus on compliance and that will result in less effort devoted to security with the ultimate result of the network being less secure. "One size fits all" model is not beneficial. *We do need some regulation to ensure effective cyber security programs are in place. However, the expanding level of regulation will adversely impact the current level of security in the sector.*
	PO4: Unless the regulation comes with very prescriptive guidelines for how actions are taken and information is to be reported, then it will just create more confusion and make it more difficult to share information. In other words, "we would be toast."

9.3.3. **<u>Third-Party Linkages</u>**. The second alternative hypothesis to explain private sector motivation to share cyber security information relates to third-party actors. According to several social network theorists, third-party actors act to build additional linkages based on their existing relationships with the two parties being linked. As theorized, their efforts are effective because they can facilitate the process of building trusting relationships. In the electric power sector, third party organizations that are well positioned to play this broker role are the trade organizations. They have technical expertise and they interact with several government bodies on a regular basis to promote industry interest. However, the answers to the first question in Table 4 provide no clear indication of the importance of these industry organizations to the cyber security network. Only one respondent highlighted the importance of having the trades present at forums, and none identified a trust-building role for the trades. While the trades may play an advocacy role in certain forums, there is no indication that they play a significant role in either sharing or fusing operational cyber security information. The resulting lack of connectivity is depicted in Figure 15.

When looking outside the trade organizations, there are clear indications that other third-party actors are important for fostering critical links. In answering the second question in Table 4, several respondents highlighted the importance of other third-party actors to help build trusting relationships. The third-party actors identified in the question are "in-between" organizations, such as the NERC and the sector coordinating council, which is comprised of representatives from both the federal government and private industry. Using social networking concepts, these third-party actors play a brokering role. Table 4 also contains the responses from federal government stakeholders, which are included to identify if their perception matches that of industry regarding the role of third-party brokers. Encouragingly, the government stakeholders understand the importance of this issue as well. In spite of the responses regarding the role of trade organizations, these responses support the second rival to Hypothesis 2B. Once again, trust plays an important role. In this case, there is evidence that firms in the electric power sector will contribute to the cyber security information-sharing network because linkage to the federal government was fostered by third-party organizations the firms trust. The goal again is to build trust between the two parties being linked by the brokers.

Table 4: The importance of third-party linkages.

Sample Question	Selected Answers
Do you think the contributions of your industry representatives motivate you to collaborate more closely with other stakeholders in your sector (e.g. ES-ISAC, and DHS) on cyber security?	*PO1: No they don't. Within the state, the CIP working groups are insular*
	PO2: Yes. It's important to see industry buy-in and to see that others are taking part.
	PO3: Unknown.
Do you think that the actions of organizations like ES-ISAC, sector working groups, or other third-party actors facilitate your interaction with the federal government actors? If so, how? would impact your current level of participation in the national cyber security network?	*PO1: Yes, they form groups you can trust. They generate working relationships. Need to keep fostering relationships*
	PO2: Yes, building relationships and networks is important. Being included externally does a lot for all the stakeholders. It helps overcome other shortfalls and disincentives to cooperate.
	PO3: Yes, we do rely on third-party linkages.
	PO4: As a company, the actions of these third parties have facilitated interaction.
	GO1: Sector working groups do facilitate interaction with private sector. Interviewee participates in the Regional Coordinating Council. Helps build relationships and trust.
	DOE: Speaking of owner/operators: ES-ISAC definitely facilitates interactions at least with their current cyber security leadership in place. They are pulling together both sides. Another example is the cyber security POC at NARUC- she educates the various utilities commissioners
	NERC: ES-ISAC tries to facilitate the conversation between industry and DOE/DHS. They will also move reports up to USG as advisories are produced. NERC may also produce a larger report or conduct face-face meetings with DOE and DHS. *Other groups- there is an Energy Sector Coordinating Council that works well with oil and gas sectors but is tremendously dysfunctional in the electric sector. It never really stood up to coordinate like the other councils have done. Someone is trying to change this by making CEOs the lead for the council. It is supposed to generate the policy discussions to work issues and engage USG to reconcile policy issues. The trade associations are also supposed to be part of the council.*
	DHS: Yes they do. Third party actors are less concerned about liability.

9.3.4. **Additional Observations.** In spite of federal efforts to formalize the cyber security regime, my observations suggest that information-sharing will continue to occur in ad hoc forums and through individually initiated networking efforts. Individual, informal networks may be the most resilient aspect of the overall information-sharing network. There is a clear response from industry that more interaction is better than less. Interviewee comments contained in Table 5 show their desire for continued interaction with other stakeholders. The encouraging aspect of these responses is that no one is arguing for less government involvement in cyber security efforts. This attitude creates a valuable opportunity for the federal government to take an active role in trust-building measures. Such measures could include table-top exercises, organizing meetings to share best practices, or implementing pilot technology projects with private sector participants.

A less encouraging observation is that private sector operators have the impression that federal agencies have access to privileged or classified information that the agencies should be sharing with industry. This is an expectation that federal agencies must contend with. Either the impression is false and must be countered, or greater efforts must be made to provide useful information. If such information is not provided to the private sector, they will most likely reevaluate their contributions and determine that the costs outweigh the benefits.

Table 5: Additional responses highlighting the importance of trust.

Sample Question	Selected Answers
What actions could the DHS NCSD, DOE, and NERC take to increase your incentive to work with them and others in the area of cyber security (for example, how to resolve the compliance/ security dilemma)?	*PO1: The NERC should allow the US government to share information, build relationships, and be more involved in NERC led CIPC meetings. For example, CIPC can let DHS/DOE get more time on the agenda to share information on current and planned initiatives. The associations work to manage the agenda. They force the guidelines to be watered down because they are concerned about compliance risks. Regarding DHS- We need better coordination between DHS protective security advisors and the critical facilities to do more accurate assessments. DHS training resources for cyber threats against control systems.*
	PO2: A lot of the industry felt burned by Aurora. When Idaho Labs released the video to the media, it set relationships back and widened the chasm between USG and industry. It was supposed to be a secret study and seemed to have been released for publicity purposes. In the end, it damaged trust. Take baby steps. Meetings are important for getting parties to talk. Table-top exercises are productive. They help people learn from one another. Need more actionable products. We understand that intelligence has to be bi-directional. DHS needs to simplify their structure to the industry so they understand who does what. There needs to be less re-organizing.
	PO3: Maintain control of information- we should be able to submit and disseminate to only a controlled environment. Ensure those who receive information have been vetted. Not sure if there is a process for how the recipient list is managed.
	PO4: Conduct more conference and interactive forums like the ICSJWG, and maybe webinars. Provide organizational perspective on what they want industry to share. Allow industry to give feedback on what the government thinks they are providing us. "We have this website" is not a solution
	GO1: At DHS, there seems to be too many political appointees involved in cyber security. Too many people in control systems and infrastructure security that do not have a solid reputation within the electric sector. DHS seems to have run roughshod over industry and put out products that don't add value. PMAs should be the source of information to DHS, in lieu of the labs, regarding threat and security postures. DHS has never consulted us on matters. DHS has no operational experience to stand on.
	Vendor 1: Government groups, DHS, DOE, ISACs, ICSJWG, etc. have positioned the vendors in a role, for the most part, as looking from the outside in and always trying to position themselves as a key and valuable contributor to any possible solution. DOE seemed to have the best success in creating an environment where all groups came together and defined the Energy Roadmap, to-date it is the only roadmap that had direct participation from the Vendor community.

9.4. **Summary and Discussion.** Discerning the fundamental motivations for any form of self-regulation is a difficult task, one complicated by the diverse nature of the public and private sector actors in the electric power sector. As identified in the NIPP, the framers of the current cyber security architecture are relying heavily on the willingness of private industry to guarantee their own security and to partner with the federal government in coordinated responses to significant events. The results presented in this research force us to question the assumptions contained in the NIPP regarding empowerment. Partnering with the private sector to develop the plan may lead to a greater or more lasting willingness to contribute to its execution. However, the increased interaction may be an indirect effect of partnering. The direct effect may be improved trust, which could lead to increased private sector motivation to participate in national cyber security efforts.

The immature nature of research in the field of national cyber security policy makes research in the area challenging. Additional evidence of cooperation with federal cyber security efforts could come from direct observation of incident reporting and information-sharing, the assessment of security measures already in place, and the observed participation of the companies in cyber security exercises. However, due to confidentiality measures implemented to encourage use of the incident reporting system and security inspections, these actions cannot be directly measured. The only way to validate interview responses is to match them with the responses of those at other ends of network linkages and to observe the respondents' participation at industry events.

Also, this research does not assess the *effectiveness* of the collaboration. The study is a snapshot of the cyber security regime and cannot assess the lasting impact of information-sharing. In the absence of publicly available statistical data on cyber security issues, case study analyses of the key stakeholders in each CI sector will continue to be the prominent research method to improve our understanding of the motivations to share cyber security information (Hare 2009). Lastly, this research cannot address the barriers to providing operationally relevant information to private firms. Clearly, detailed information on cyber threats would be beneficial to cyber security professionals at electric power firms who must argue for robust security measures. In the absence of previous attacks on their operations, there is no other way to develop an assessment of the operational risk being taken by the firm. Unfortunately, an analysis of the procedures necessary to disseminate such information, were it available, would require an in-depth, and most likely classified, analysis of the intelligence community.

In Part IV, I will combine the results obtained in this chapter with those from Part II to develop general conclusions from this research. Though each problem I researched is unique, there are commonalities between the two. The commonalities can be used to show relationships between the private sector components of cyber security I have explored through this dissertation. The conclusions I present will also inform public policy measures to improve our nation's security in this important domain.

Part IV

Public Policy to Improve National Cyber Security

10 Conclusions and Policy Implications

10.1. **The Character of the Public Policy Problem.** In the introduction to this dissertation, I highlighted two incidents that have drawn attention to the nation's lack of security in the domain of cyberspace. The first incident was the breach of the systems responsible for diagnosing maintenance problems during flight testing of the new Joint Strike Fighter (JSF). The JSF is designed to replace the F-15 and F-16 as the nation's premiere air defense fighter. Knowledge of the flight characteristics of this aircraft would greatly benefit potential adversaries as they attempt to develop missiles and other counters to the weapon. Another cyber security incident that has implications for the nation's security was the penetration of the electric grid by malicious actors who left behind software capable of disrupting power (Gorman 2009). These critical cyber security breaches demonstrate that essential investments necessary to secure the nation in cyberspace and to respond to a national crisis have not effectively occurred.

In Chapter 2, I presented a definition for the public good of US national cyber security to focus the dissertation on those cyber security issues that should be considered issues of national security. I proposed the following definition of the public good of national cyber security:

> The state of being in which the populace, governing institutions, and critical infrastructure are not threatened by
>
> - attacks and intrusions through cyberspace, by either state or organized non-state actors, against government and select other information systems to gain knowledge of a national security value
> - attacks and intrusions through cyberspace, by either state or organized non-state actors, against critical infrastructure systems (privately and publicly owned) to degrade or disrupt such systems creating a national security crisis

There have been several recent efforts to securitize the potential threats from both these types of attacks. The most concrete securitization efforts can be found in proposed legislation. In June of this year, the House passed the Grid Reliability and Infrastructure Defense (GRID) Act. This bill is intended to protect the bulk-power system and electric infrastructure critical to the defense of the United States against cyber security and other threats and vulnerabilities (Markey 2009). While the debate continues on Capitol Hill regarding the costs and benefits of additional regulatory measures to secure the nation's critical infrastructure from cyber attacks, federal agencies, such as DHS and the FBI, continue to rely on voluntary private sector actions. The Obama administration may have the constitutional authority to invoke extraordinary emergency measures to direct much stronger cyber security actions if the nation is truly at immediate risk from threats in the domain. However, this and all previous administrations have been unprepared to make this policy move. Instead, the executive branch has chosen to rely on the current, self-enacted cyber security measures in most of the critical infrastructure sectors. Perhaps recently proposed legislation such as the GRID Act will force a more involved role for federal, state, and local governments on a day-to-day basis. Whether considering additional regulations or continuing on the current path, any public policy measure would benefit from a better understand of the policy problem at hand.

Based on the results of this research, I have characterized the public policy problem in the following way:

- Due to the inherently commercial nature of the cyber domain and the ease with which an attacker can reach their target, the federal government cannot effectively conduct the necessary actions to provide for the public good as just described. Therefore, the vast majority of this public good must be provided by the collective action of private commercial organizations.
- The collective actions necessary to provide for the public good cannot be observed by anyone beside the implementers. The beneficiary of the good, the general public, cannot get a sense of their level of security and therefore cannot advocate for improvements in cyber security at firms within the CI sectors. As a result, government oversight and

enforcement of cyber security measures cannot be easily achieved because investment is not easily measured nor understood by regulators and others. In addition, coordination of the action between all actors cannot be easily achieved, since they also cannot easily observe each others' actions. These factors lead to a disincentive to invest at any level, or to make potentially inefficient investments (like buying three tires for a car; anything short of four is wasted).

- There is potential for firms in all CI sectors to free-ride in the information-sharing network, since the government is required to provide information to all components of the nation's critical infrastructure regardless of the contributions made by the recipients. DHS and the sector-specific agencies are expected to support all firms in their sector, whether or not the firms reciprocate in any way. In other words, the government cannot make the dissemination of information important to the nation's cyber security a club good.
- Attainment of the goal of national cyber security cannot be easily identified, and the efficacy of cyber security measures cannot be easily observed and quantified. For example, an effective attack may be kept hidden from view if there is no physical manifestation of the attack, such as power going out. As with all security problems, in the absence of an attack, the effectiveness of security measures cannot be assessed

unless the attacker confirms that the measures were an effective deterrent to an attack. The threat is continually adapting to current measures, so the goal will continually shift.

All of these factors lead to problems with ensuring both the adequate level of investment and the sharing of information necessary to improve and adapt current investments to the evolving threat. Therefore, it is critical that cyber security investments and the communications networks be both robust and highly adaptive. To achieve this end, rapid information-sharing during crises is critical.

The interconnectedness of the nation's critical infrastructure, coupled with the voluntary nature of cyber security measures, creates great potential for negative externalities or for decisions resulting in costs to the public that are related to national security in cyberspace. This research examined the challenges the federal government faces in fostering private sector contributions to the nation's security to reduce and ultimately remove such potential externalities. With a foundation for understanding the public policy aspects of the national cyber security issue, this research tested hypotheses related to both cyber security investment and the sharing of cyber security-related information. The results of each assessment are contained in Chapters 6 and 9, respectively. For the rest of this chapter, I will summarize and synthesize my conclusions from this work. In section 10.2, I will highlight the important findings from using an agent-based model to explore the dynamics of investing in cyber security in a knowledge-intensive sector of critical infrastructure. A better understanding of the interdependent nature of this important decision for the firm should help policy makers craft more effective policy to encourage effective investment. In section 10.3, I present conclusions regarding the challenge of sharing relevant information that can improve security measures and help the nation respond quickly to crises in cyberspace. This portion of the research used a qualitative case study approach to focus on motivations for sharing information in a complex social network of public and private sector actors. Finally, I will discuss the interrelationship between the two components of this cyber security issue and how the mixed method approach strengthens the results of both parts.

10.2. **Conclusions Regarding Cyber Security Investments in an Interdependent System**. For this research, the problem of improving cyber security investment levels was modeled as an interdependent decision problem. As several previous researchers have shown, interdependent binary choices characterize many security decision-making events in the real world. This work can expand understanding of the interdependent nature of these phenomena when the decisions being modeled occur within a networked environment. Utilizing an agent-based modeling approach and an empirically bound set of parameters, this research has found that the nature of the interaction network may influence the decision process in important ways.

Before discussing the conclusions regarding the influence of the interaction network and the ability to generate critical investing coalitions, it is important to assess the utility of using an agent-based model to explore the IDSI problem. This issue was addressed with Hypothesis 1A: *The significant features of the IDSI model hold when introducing into the model the network aspects of interaction between firms, an endogenous risk of direct attack, and the potential for non-rational decision-making behavior*. This hypothesis related to the employment of agent-based modeling techniques to test a theory, not to testing a theory based on observed behavior. However, all components of the IDSI theory were present in the agent-based model environment used for this research. The relevant parameters and decision-making algorithms from the Heal and Kunreuther model were all incorporated. All expected equilibria were achieved, and cascading and tipping did occur.

The results from the agent-based model suggest that the theory is robust in some dynamic environments. When agents making a security investment decision are endowed with two-hop vision, they behave in a manner similar to having perfect vision across the system. This similar behavior most likely results from the fact that the scale-free network within which these actors interact effectively brings the agents closer together. Few agents are separated by more than two degrees. When the agents are myopic, meaning they can only assess the actions of their direct neighbors, the network acts to reduce the perceived risk within the system, but it also appears to reduce the cascading and tipping effect of changes in the investment state. Two significant findings for myopic agents relate directly to the scale-free nature of the network. First, the central actors in a scale-free network appear to create the largest total risk to the network, based on the behavior of the agents in the model. When the central actors invest, many other actors that are only connected to them are induced to invest as well.[58] However, the central actors also appear to experience the largest individual risk from the network around them. In other words, the central actors in this environment have the largest disincentive to invest. Also, non-rational investment decisions can lead to system-wide behavior not predicted by the theory. This research demonstrated that it could be possible for non-rational behavior to impede tipping and cascading that would otherwise occur. These results highlight the importance of considering the true nature of the investment decision, the ability of actors to perceive the actions of

[58] This behavior may seem to contradict observations made earlier regarding the behavior of peripheral and central actors. In the absence of an initial coalition, some peripheral actors may choose to invest while others do not. However, a critical coalition of central actors will convince the remaining peripheral actors to do so.

others, and the nature of the threat. If actors cannot effectively account for the actions of all others in the system, their behavior may generally conform to the theory but the system may reach much different equilibria than expected for a given set of parameters.

Once I determined that the agent-based model developed for this research could model the IDSI problem as theorized, I turned to an analysis of the effect of coordinating investment behavior. The effect of coordinating behavior was tested with Hypothesis 1B: *Coordinated action of a small coalition of firms in a CI sector can tip a sector toward full investment. This action is effective in the face of a significant threat of security breaches emanating from with the sector*. Using empirically generated parameters, this research demonstrated that initial coalitions of a small collection of central actors can become critical coalitions under certain conditions. Coordinated investment behavior can lead to a state in which all actors in the system invest for a broader range of threats.

However, the interaction environment can influence the ability to generate critical coalitions. For example, the counter-balancing forces between the central and peripheral actors in a networked environment make it difficult to coordinate investment in an initial coalition of central actors that does not tip all peripheral actors to a state of investing by T_2. It is also important that the critical coalition quickly tips the system toward full investing so that individual agents do not make investment decisions based on faulty risk calculations and the system ends up in an inefficient, mixed equilibrium. These results suggest that if the agents can be assumed to be myopic, efforts to produce critical coalitions should focus on the actors playing a central role in information-sharing networks. Also, the investments of the central actors may need to be mandated as the rest of the system fully responds to their actions. While policy could be targeted toward peripheral actors, most if not all actors would be required to be in the critical coalition, otherwise they may not be able to change the behavior of the central actors and generate the necessary tipping in the system.

These conclusions lead to at least three implications for policy considerations. First, the goal of policy must be a very high level of system-wide investment (as near 100 percent as possible) to avoid mixed equilibria that are ineffective in countering threats that pass easily through the system. This high level of investment should become self-sustaining, due to the previously mentioned difficulties of effectively monitoring investment levels. Second, it may be possible to overcome the challenge of empirically measuring investment levels across the system and the probability of attacks from cyber threats, as long as the actions of the central actors can somehow be signaled to the rest of the system. As shown in Chapter 6, Figure 13, the initial coalition of all prime contractors led to system-wide full investment for all values of p_{ji} when agents were myopic. In other words, in cases where the security investors can be expected to have myopic vision (i.e., considering only the decisions of those with whom they interact most closely), it appears that the central actors have such a strong influence on the actions of others that the central actor can tip all others to invest regardless of whether the threat from attack is very low or very high. Finally, policy must always consider non-rational behavior. According to the results from this research, non-rational behavior can significantly impact the ability of an initial coalition to drive system-wide investing if those who had invested in previous periods are allowed to reduce or cancel their investment in spite of favorable investment conditions.

10.3. **Conclusions Regarding Information-sharing in a Complex CI Sector**. The challenges of cyber security are unique in each sector of the nation's critical infrastructure. For example, the unique requirements for securing control systems in the electric power sector leads to an imperative to incorporate the expertise of at least ten stakeholders in the sector. The diverse agendas of these stakeholders lead paradoxically to the challenge of creating an information-sharing network amongst the actors that adds value to each stakeholder. However, as the sectors become increasingly inter-dependent, mutually supportive solutions must be found. Of prime importance is promoting information-sharing amongst the private owner/operators in all CI sectors who are on the front line in cyberspace. Without their contribution, such as reporting cyber attacks on their systems, the federal agencies responsible for securing the nation in this expanding domain are at a distinct disadvantage in mitigating future threats.

This research has argued that social networking theory provides a useful framework for addressing this information-sharing challenge. To determine if it was appropriate to use networking theory in the electric power sector, I began the analysis with Hypothesis 2A: *Stakeholders in the electric power critical infrastructure sector participate in an information-sharing network to exchange information relevant to cyber security.* As could be expected, there was not a common perception of the relative relationships in the network. Specifically, there were differing views of the structure of the network and who the central actors are. For example, DHS sees itself as a central actor; however, other stakeholders do not look to DHS to play a leading role. Such misaligned perceptions could cause communications problems during a crisis, as there would be confusion regarding where to look for direction. In addition, I found several principal-agent issues between owner/operators and information-fusing organizations. For example, private firms were concerned about compliance penalties when sharing information with the NERC. Also, DHS and DOE had to anonymize reports when sharing them with NERC. Nevertheless, in spite of several principal-agent and other barriers, I found, through observation and interviews, that there is a communication network in the electric power sector that shares information relevant to cyber security. With this theoretical basis, I assessed the claim contained in the National Infrastructure Protection Plan that the private sector is motivated to cooperate with the federal government and with each other because it has been empowered to create the nation's plan of defense. The specific proposition I tested is contained in Hypothesis 2B: *Private firms in the electric power sector will contribute to the collaborative, information-sharing network because they and their industry representatives contributed to the development of the information-sharing protocols.* In addition, I considered several rival hypotheses, such as the desire to avoid government regulation and the bridging actions of third-party actors, as reasons to explain cooperation. In general, I found that the motivation for the private sector to participate in this network couldn't be explained through the theory of empowerment as it is commonly understood. According to the results obtained from interviews with a small sample of electric power sector operators, the companies do contribute to the national cyber security regime and they are proud of their contributions. They do appreciate that it is an important contribution they could make for homeland security. But why do they do so? None of the hypotheses individually appears to provide the clear answer. The answer to the question may be derived from the responses regarding empowerment and third-party actors. The common theme between the respondents' answers is the importance of trust-building measures. Bringing organizations together, whether to develop incident-response plans or to discuss other issues, increases their interaction and that leads to greater trust between cyber security professionals at all locations. The idea that they cooperate to avoid further government regulation may be a red herring. Yes, they are always concerned about government regulation, but not because more regulation will directly impact their motivation to cooperate.

These findings have important policy implications. The actions undertaken by DHS with the intent to empower the private sector nevertheless have a positive impact on the cyber security regime. The simple act of bringing the private and public organizations together in working groups increases interaction and helps to build trust between stakeholders. However, the perception remains that the government is not disseminating important intelligence it has received regarding threat actors. DHS and the sector-specific agencies must make a concerted effort to demonstrate that they are being forthcoming with all available intelligence.

10.4. **Common Factors.** In addition to the conclusions that are specific to each portion of the dissertation, there are three common themes between the two sets of research findings; the synergistic effect of improvements to either component, the need to reach a tipping point, and the potential for free-riding. I will discuss each of these themes, and the strength of using a mixed-method approach to explore them, in this last section.

Improvements in the amount and type of information shared between all stakeholders should improve the cyber security investments of owner/operators in all CI sectors. Most information disseminated by fusion and response centers, such as ICS CERT and the ES-ISAC, relates to current cyber threats and best practices. This information may be necessary to conduct emergency responses and it may be specific only to certain sectors or cyber system technologies. However, in the aggregate, such information can help organizations facing cyber security investment decisions better evaluate their risks and benefits from investing. As this mixed-method research supports, an increased understanding of how and under what circumstances stakeholders share investment information is also beneficial for addressing both components of the cyber security challenge. Not only does it show where communication should be improved, it also improves the ability to model the investment decisions. For example, actors in the DOE enterprise share investment-related information freely (i.e., similar to agents with perfect vision). On the other hand actors in the private sector share investment-related information infrequently, and only with trusted partners (more like myopic agents). This information can be used to tailor an agent-based model to each CI sector or subsector.

Secondly, there is the potential for a tipping point, or critical level of interaction, to create self-reinforcing conditions in both cyber investment and information-sharing. In the case of the IDSI problem, the critical coalition will drive the system to a full state of investment. I discussed this concept of a tipping point earlier; however, there is also the potential for a tipping point regarding the information-sharing network. In this case, a tipping point would refer to the sharing of sufficient information to generate useful analysis that is disseminated back to the system. The information these analysis centers provides to the private sector is often based on reporting originally received from the private sector. If the analysis provided to the private sector by the analysis centers does not help them improve their day-to-day cyber security operations or support their investment decisions, the private sector will be less interested in interacting with the analysis centers and seeking out their expertise. Therefore, if reporting can be sustained at a sufficient level to provide useful analyses, there is a much better chance of promoting more communications. Modeling this tipping point concept is extremely difficult in qualitative analyses. However, the analysis conducted with the agent-based model can help researchers understand the influence this phenomenon has on an entire CI sector. For example, it helped me understand the true significance of interview responses in the case study as they related to expectations of useful cyber security information from government agencies and the ES-ISAC.

Lastly, there is potential for actors to free-ride on both investments and the information-sharing efforts of others in their CI sector. In states of mixed equilibrium in cyber security investments, those who are not investing receive potential benefits from those that do invest if the investors are able to reduce the system-internal risk of attack to all in the system. In the basic IDSI model, this is not to be expected because it is assumed that investments only protect the firm from attacks that are launched directly against their systems, not through channels used to interact with others in their sector. However, it is more likely the case that cyber security investments undertaken by any actor in the system will reduce the ability of a malicious actor to move freely within the system once they have penetrated one actor's outer defenses.[59] The problem of free-riding on the information-sharing actions of others in the system is greater. Since the federal government cannot withhold important information, everyone in all CI sectors can receive it regardless of the amount of information they have contributed themselves. As stated earlier, the federal government cannot make their cyber threat

[59] A dynamic opponent will, of course, counter the desire to free-ride. In other words, if most actors in the system have invested, the malicious actor may decide to focus their attack on those who have not chosen to do so. Once the non-investors begin facing concerted attacks on their system, they may quickly change their investment decision.

information a club good. They are obligated to provide information designed to secure the CI sectors at no cost. These three common factors demonstrate the importance of considering both components of the cyber security challenge during policy formulation. This point will be further discussed in the closing chapter.

11 Policy Recommendations and the Future

11.1. **The Role for Public Policy.** I chose the defense industrial base for this research because it is a knowledge-intensive sector of critical infrastructure, and because data existed from which to construct an information-sharing network topology for an agent-based model. Also, there is a clear threat to the sector from cyber espionage conducted by competing firms, nation-states, or other malicious actors. However, the findings in this research should have public policy implications for any situations in which the IDSI problem confronting the sector is similar. Such situations include environments that approximate a scale-free network of interdependence, and those in which the agents can be expected to have difficulty assessing the investment decisions of others in the system. This might include other sectors of the critical infrastructure, such as utilities, or other sectors of the economy, such as biotechnology.

I chose a sector different from DIB to explore the information-sharing issue for two reasons. First, the analysis of the electric power sector contained in Chapter 7 demonstrates the general diversity of cyber security challenges among different CI sectors. For example, unlike in the DIB, the focus of cyber security is not on the security of information in the firms' IT systems. As the description of the sector in Chapter 7 showed, the emphasis in the electric power sector must be on the security of the control systems that govern the generation and distribution of electric power across the nation. This functional and technological difference between security goals creates an additional layer of complexity to the cyber security challenge. Second, the public and private composition of the electric power sector and the need to share cyber security information immediately during a crisis creates a more complex information-sharing problem than in the DIB. In the DIB, the vast majority of information regarding weapons systems development resides at the contractor facilities. Also, the DIB does not have an immediate need to share information among firms in a crisis, since most of the information is related to research and development. Clearly, the challenge of sharing information related to cyber security in the electric power sector is greater than within the DIB.

Though I chose two different sectors with which to research each component of cyber security in our nation's critical infrastructure, it does not mean the two components can be addressed independently. In spite of the differences between the two sectors I have just highlighted, the conclusions presented in Chapter 10 show that policy makers must consider both components of the cyber security problem in tandem. In fact, the interrelated nature of these two components holds the greatest implications for the development of public policy to address either, or both. For example, regulations designed to increase investment will have the unintended consequence of reducing information-sharing if it is not well tailored to each sector. In other words, because of the unique aspects of each sector, any public policy measures designed to improve cyber security must account for each sector's uniqueness, so that measures designed to address one component of the problem do not exacerbate the other. For example, regulations requiring infrastructure operators to implement additional security measures and incident reporting that are standardized across all CI sectors may increase the compliance risk in some of the sectors, and thereby discourage reporting of significant incidents. This unintended consequence, especially in sectors where the necessary actions are conducted primarily by the private sector, may have a greater impact on provision of the public good of national cyber security than that which was intended. Another example could be the implementation of more stringent reporting requirements. Again, if it is not tailored to each CI sector, the intended benefit of increased information-sharing may be outweighed by the reporting burden that would leave fewer resources available for conducting security operations. Although it is imperative to consider both components in tandem, I will consider public policy implications specific to each component.

11.2. **Policy Options to Improve Interdependent Cyber Security Investments**. Regarding cyber security investment, the most significant implication of the findings from this research is the difficulty of targeted intervention, or centrally coordinated behavior, to induce tipping in the interdependent security investment decision.[60] In cases where actors can see and assess others' actions (e.g., perfect or two-hop vision in a scale-free network), a small initial coalition has little chance of influencing the investment state of the system. Even in cases where the agents are myopic, an initial coalition of central actors may choose to divest in subsequent periods if insufficient numbers of other actors choose to follow their investment decision. In the literature review, I described several policy alternatives that have been suggested in the literature to address underinvestment in cyber security from the standpoint of public goods. However, the results from this research support two actions that might be considered practical to improve system-wide cyber security investments.

First, there is potential for policy to improve security investments through contract language. As Heal and Kunreuther (2005) suggest,

[60] The public policy discussion regarding the defense industrial base has been updated from a previously published article in the International Journal of Critical Infrastructure Protection.

standards can be incorporated into contracts that require a minimum level of security. In the case of the defense industrial base, for example, major weapons contracts could require a standardized level of cyber security before a candidate firm is selected as the prime contractor.[61] This arrangement would signal to potential subcontractors that they would be entering into an interdependent data-exchange network without incurring additional risk. This information might motivate them to invest as well. This measure would also be an example of creating an enforced, critical coalition of the central actors in the system. Creating a coalition whose actions are somehow visible to other actors is necessary to achieve the influential effects highlighted originally by Schelling (1973). The language must also allow for periodic inspections of these security measures by a qualified cyber security expert. Without the possibility of periodic inspections, there could be a strong incentive to begin free-riding in subsequent investment periods if the system has not reached sufficient investment levels.

Second, absent the federal government's imposition of contract standards, any actions that would improve the common knowledge of current investment practices would help firms accurately estimate external risks (i.e.,

[61] It is often suggested that the federal government should direct greater security in office productivity and general IT security products that it purchases. However, the federal government does not seem to be a large enough customer of these products to have the necessary influence. On the other hand, the US government is the only customer for most major weapon systems and it should be able to leverage this position more effectively to influence the actions of prime contractors regarding their cyber security programs.

system internal) to their operations that are incurred by sharing technological information in their contractually based interaction networks. Trade associations or other organizations could promote best-practice sharing and provide insights into current security measures to reduce costs and increase confidence that others are making effective security investments. Similar suggestions have been made by Heal and Kunreuther (2007), and Coase (1960). In the case of the defense industrial base, the major trade organizations have an active symposium and conference agenda that could be used to highlight the impact of the interdependent cyber security risk and heighten awareness among member firms that others are investing in effective cyber security.

Third, the sector-specific agency for this CI sector, the Department of Defense, can strengthen its role as a third-party broker to help DIB firms understand current threats and improve their cyber security investments. The DOD is not only a customer of the DIB, it is a partner with the DIB in the cyber security challenge. The DOD DIB Cyber Security Task Force has begun to address this issue by implementing the DOD-DIB Collaborative Information Sharing Environment (DCISE). This initiative is an excellent example of addressing both components of the cyber security problem in tandem, because the DCISE is designed to share information on threats and best practices that will improve cyber security investments (ASD[NII)/]/DOD

CIO 2010). Other sector-specific agencies could use this model to engage with firms in their CI sector.

The last two issues have important implications regarding non-rational behavior among the cyber security decision makers. As this research demonstrated, coordinating behavior that leads to cascading investment decisions may be extremely difficult when even a small portion of the actors do not conform to the expected behavior pattern. The tipping point may never be reached, given a certain set of initial parameters, if some who had at one point chosen to invest decided not to invest for reasons that did not appear rational (according to the limited considerations of the model). However, the long-term effects of this type of non-rational decision can be reduced if greater information regarding the decisions of others can reduce the probability of a non-rational decision at any point. On the other hand, some who made the non-rational decision to invest in security may actually counter the non-rational decision in future periods if they become aware that others are not investing sufficiently. Clearly, policy must account for both effects and ensure that a self-sustaining critical coalition can be achieved, under realistic conditions, if investments are regulated in a system where non-rational behavior can be expected.

11.3. **Policy Options to Encourage Greater Information-Sharing.**

Regarding the information-sharing component of the cyber security problem, the most significant policy implication demonstrated by this research is the need to foster continual engagement with all the important stakeholders. As with cyber security investments, there is a minimum threshold in the amount, and quality, of information being shared, such that participation becomes a valuable experience for all. All interviewees felt that their organization is committed to cyber security and working with other stakeholders, both public and private. However, DHS and DOE cannot rely on the current atmosphere if continued participation in the information-sharing network is not shown to be value-added for the private sector. Considering the significant barriers, such as the risk of a compliance penalty, the benefits of taking the risk must become much more tangible. But communications must occur both ways. In order for the benefits of cyber security analysis to become more tangible, the private sector must contribute relevant information regarding cyber attacks on their infrastructure. In other words, information must be shared in each direction to reach the tipping point. If the private companies see a clear informational value from participating, they will not only be motivated to continue collaboration with DHS, DOE, and NERC, but will also help build the national network and increase public-private trust. Policy options to meet these challenges do not have to be complex.

To “prime the pump,” trust in the system must be strengthened through frequent interaction. Trust cannot be mandated. The private sector is not necessarily looking for leadership or directives from the government. They are looking for facilitation and coordination of effort. Each CI sector-specific agency has a role to play. In the case of the electric power sector, it is important for DHS, DOE, and NERC to foster and facilitate the participation of the private sector actors in cyber security forums to increase trust in the system and motivate the sharing of information. Second, government agencies must demonstrate to the private sector that they are providing all available information to them. For example, DHS can provide regular progress reports regarding steps they are taking to grant key private sector personnel access to classified data. These updates can be incorporated into the agenda of all CI sector forums. It is not possible for the DHS and DOE to “over-promote” this issue because the perception that they are not sharing relevant information is well entrenched. Building trust requires continual engagement, but it is the key to improving national security in cyberspace. Other measures of empowerment that do not entail group interactions, such as allowing owner-operators to submit ideas and best practices via a web portal, may seem to be empowering, but they will most likely not lead to greater trust between stakeholders.

The policy options for addressing the issues raised in this research may seem simple, but their simplicity may be their greatest strength. Simple measures, such as fostering continual interaction, reduce the probability that they will be improperly executed or become unfunded mandates. Simple measures are more sustainable by organizations like DHS that have high turnover rates. In fact, they may be an effective way to cope with frequent turnover and the need to reestablish networks after each new personality is emplaced at DHS. Simple actions like fostering frequent interaction lead to greater familiarity between key advisors and to stronger trust in the formal and informal relationships. Stronger trust leads to greater network resiliency in times of crisis, and resiliency of the information-sharing network is necessary to be able to adapt to new threats and unforeseen events. Since information-sharing is most likely to continue to occur in ad hoc forums and through individually initiated networking efforts, national response actions to cyber threats must account for this. Individually developed, informal networks may be the most resilient aspect of the overall information-sharing network for all CI sectors. Given all the potential threat vectors and impacts on CI, the federal and local government cannot possibly expect to be on the scene at every impacted location to oversee or lead response measures. Policy makers would be wise to recognize and promote spontaneous, self-initiated networks for crisis preparedness and response.

11.4. **Future Research**. Future empirical work may extend the analysis in this research along a number of dimensions. Some aspects can be incorporated into future versions of the agent-based model or case studies of these and other CI sectors that assess cyber security partnerships.

Regarding the agent-based model, there are several extensions that could be explored with minimal changes to the coding of the model used for this research. The threat, whether from terrorism or cyber espionage, is non-random and continuously evolving. Security investments made in any period may be negated before a new investment can be planned. Future work that could forecast the threat throughout the investment period would help overcome this limitation. In addition, the cyber security threat is an adaptive actor. As Heal and Kunreuther (2003) observed, if an attacker desiring to load a bomb onto a certain airliner is unsuccessful against one target, it will most likely seek a more vulnerable one. The malicious actor in cyberspace will most likely continue to try to exploit cyber defenses until they find a weak point. While this work employed an extension that internalized the risk for each agent, the calculation was deterministic. To model a truly adaptive threat, malicious agents would need to be introduced into the model as independent actors. Another interesting extension of the agent-based model would focus more on the true impacts of limited information regarding threats and others' actions. In the absence of clear signaling, does limited information increase fear and therefore lead to a tendency to over-invest, or does it lead to a fatalistic attitude? Agent-based models could attempt to account for both potential reactions, and others. Finally, I should reiterate that the agent-based model employed for this dissertation is intended to shed light on the underlying dynamics and sensitivities of the IDSI problem. As more empirical data become available, the model should be refined to provide a picture that is as accurate as possible for any cyber security problem that can be modeled from an IDSI perspective.

In addition to improvements in the agent-based model, I recommend that future research consider two other issues raised by this study. First, future research could explore ways to overcome the problem of directly observing cyber security while still providing for necessary confidentiality guarantees. How can cyber security actions be signaled to others that depend on the actions? Since physical security occurs at the physical perimeters, it can be signaled to others without inadvertently disclosing other actions occurring within the facility. However, cyber security is conducted at the heart of the enterprise, thus it is difficult to observe and measure without risking the unintended disclosure of other sensitive information. Future research could explore ways to create observable indications that do not require intimate access to a firm's IT and control system networks. Second, research could consider ways to internalize the positive security externality created by a robust cyber security investment. Although generally difficult to measure, increased understanding of the public good nature of cyber security by private actors may counter-balance the structural barriers described in this research. The private sector needs to have a better understanding of how their actions, and inactions, are directly related to national security. It would be useful if future research could help quantify this factor for the cyber security experts at firms in each CI sector. My research indicated that many of these actors do appreciate the fact that they have an important role to play in securing the nation. With a clearer understanding of the impact of their actions on national security, they could use such information to help advocate their efforts to their leadership and stockholders.

11.5. **Closing Thoughts**. As Goodman and Lin (2007) conclude in their recent assessment of the state of cyber security research, the problems of cyber security will be with us for a long time. Even if technological solutions can be found to negate many of the current threats, the characteristics of the cyber security problem for the nation's critical infrastructure suggest that better technology will never be sufficient to secure the nation. The nature of the IDSI problem shows that there will always be a strong disincentive to invest in security solutions as long as the potential for negative externalities is created within the system. The difficulty of maintaining trust and the requirement for the federal government to provide information to all regardless of their contributions of information suggest that there will always be problems motivating the private sector to share information about attacks on their cyber systems. While the search for technological solutions continues, organizational and economic issues must be immediately addressed to improve the security and resiliency of our nation's critical infrastructure. My hope is that this work provides some insight into important aspects of the cyber security problem, motivating the private sector to secure their cyber systems in support of national security and to contribute to the cyber security information-sharing and response networks. With this work, I also hope to advance the utility of two important methodologies for understanding a broad class of social-decision problems, agent-based modeling and social network analysis. Finally, a greater understanding of the motivations of private sector actors will lead to a better understanding of possible cyber security roles for other government agencies, such as the Department of Defense and Department of State. As nation-states gain tools that are being exploited by criminal elements, activities in cyber space may become critical components of diplomatic or military operations. This changing dynamic will have great implications for national cyber security. It may even lead to significant shifts in the balance of the international system, as developed nations become more dependent on cyberspace for their economic and social affairs.

APPENDIX A

PARTIAL PSEUDO CODE FOR AGENT-BASED MODEL

Partial Pseudo Code

```
Check neighbors investment decisions
    For all network neighbors of DIB Agent i
    If neighbor is not investing, increment counter
    Return counter //counter in below equation

Assess risk due to externality
    For j = 0 to counter-1
        $y = prob2 * (1-prob2)^j$
        $z = z + y$
    External = loss * z
    Return external// used below

Determine whether investing in security is feasible
    If cost < Prob1 (Loss - external)
    Decision turns to true
    Return decision

Make investment switch
    Invest = decision //This only switches after everyone has made their decisions with
    current settings to avoid path dependence.
```

.

APPENDIX B
INTERVIEW QUESTIONS FOR ES SECTOR OPERATORS

General Cyber Security

1. Please describe how your firm's cyber security measures were primarily developed (e.g., by trade association, consultants, in-house expertise).
2. Are the NERC CIP standards your primary guidance?
3. Are you familiar with the contents of the Electric Sector Specific Plan annex to the National Infrastructure Protection Plan?
4. Do you have separate cyber security systems and/or divisions for IT and SCADA?
5. Is your SCADA network security conducted by a sub-contractor?
6. From your viewpoint, what is the role of the ES-ISAC?
7. From your viewpoint, what is the role of the ICS CERT regarding cyber security?
8. What do you feel motivates your company to share information with the ES-ISAC regarding your cyber security posture and attacks on your systems? How do you see it to be in your company's interest? Please rank order multiple reasons.
9. What do you feel motivates your company to share information with the DOE and DHS regarding your cyber security posture and attacks on your systems? How do you see it to be in your company's interest? Please rank order multiple reasons.
10. Did you or your organization play a role in developing the cyber security information sharing procedures for your sector?
11. If so, do you think that your organization's contribution motivates you to collaborate more closely with other stakeholders in your sector (e.g. ES-ISAC, DOE, and DHS) regarding cyber security?
12. Did your trade organization/s play a role in developing the cyber security information sharing procedures for your sector?

13. If so, do you think the contributions of your industry representatives motivate you to collaborate more closely with other stakeholders in your sector (e.g. ES-ISAC, DOE, and DHS) regarding cyber security?
14. What disincentives/barriers do you have to sharing cyber security information with other stakeholders? Do you consider it easier to share with some more than others?
15. Do you think that the actions of organizations like ES-ISAC, sector working groups, or other third-party actors facilitate your interaction with the federal government actors? If so, how?
16. What actions could the DHS NCSD, DOE, and NERC take to increase your incentive to work with them and others in the area of cyber security (for example, how to resolve the compliance/security dilemma)?
17. What do you see as the best relationship/division of responsibilities between DHS and industry operators in the electric power sector in the area of cyber security?
18. What do you see as the best relationship/division of responsibilities between DOE and your sector in the area of cyber security?
19. Are you concerned about the possibility of restrictive government regulations in the area of cyber security? If so, how much so and how do you think that would impact your current level of participation in the national cyber security network?
20. Are you aware of current proposed legislation? How do you think they will impact information sharing?
21. Do you ever speak directly with other operators about your specific security measures (i.e., to the degree that you inform each others' investment decisions)?

<u>Additional Questions (optional)</u>

22. Does there appear to be accountability or an instrument to enforce the measures your sector has implemented (e.g., do you rely on self-enforcement)? Do you feel your company is held accountable to anyone for compliance/cooperation? If so, how so and to whom?
23. Do you ever find yourself in a position of conflicting loyalties? For example, have you ever had to defend cross-sector working groups or DHS requests/actions to your parent organization?

APPENDIX C

External Reader

Dr. Greg Rattray

As a visiting scientist for Carnegie Mellon University, Dr. Rattray brings an exceptional record in establishing program strategies for cyber security initiatives across both the government and private sectors. He has led policy formation, operational innovation, and human capital development in a variety of large and medium enterprises in the Department of Defense and U.S. Air Force.

From 2002 to 2003, he was an Air Force Fellow serving on the President's Critical Infrastructure Protection Board. During his tenure he was a key contributor to the President's National Strategy to Secure Cyberspace and served on the White House team for legislation and policy on the establishment of the Department of Homeland Security. He also established the Cyber Conflict Studies Association to ensure U.S. national efforts were guided by a deeper well of intellectual capital with over 200 individuals from private industry, think tanks, government and academia.

As the Director for Cyber Security on the National Security Council staff from 2003 to 2005, he led national policy development and NSC oversight for cyber security to include the Executive Order on Information Sharing, Homeland Security Policy Directives on Critical Infrastructure and Incident Response, the establishment of cyber security roles for the Department of Homeland Security, and interagency responsibilities in the National Response Plan.

Dr. Rattray is a Full Member, Council on Foreign Relations, since 2002, and a member of the Cyber Conflict Studies Association Board; InfraGard National Advisory Board; and the Armed Forces Communications and Electronics Association. He received his Bachelor's Degree in Political Science and Military History from the U.S. Air Force Academy; a Master of Public Policy from the John F. Kennedy School of Government, Harvard University; and his Doctor of Philosophy in International Affairs from the Fletcher School of Law and Diplomacy, Tufts University, with distinction. He is the author of the seminal book *Strategic Warfare in Cyberspace*.

BIBLIOGRAPHY

BIBLIOGRAPHY

Allison, Graham T. 1969. Conceptual Models and the Cuban Missile Crisis. *The American Political Science Review* 63, no. 3: 689-718.

Anderson, Ross, and Tyler Moore. 2006. The Economics of Information Security. *Science* 314, no. 5799 (October 27): 610-613. doi:10.1126/science.1130992.

APPA. 2007. *Public Power: Shining a Light on Public Service*. Fact Sheet. American Public Power Association, December. http://www.appanet.org/aboutpublic/index.cfm?ItemNumber=429&navItemNumber=20955.

Arquilla, John, and David Ronfeldt. 1993. Cyberwar is coming! *Comparative Strategy* 12, no. 2: 141. doi:10.1080/01495939308402915.

ASD(NII)/DOD CIO. 2010. Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA)
Activities. Department of Defense, January 29.

Assaf, Dan. 2008. Models of critical information infrastructure protection. *International Journal of Critical Infrastructure Protection* 1 (December): 6-14. doi:10.1016/j.ijcip.2008.08.004.

Auerswald, Philip. 2006. Complexity and Interdependence: The Unmanaged Challenge. In *Seeds of disaster, roots of response : how private action can reduce public vulnerability*, ed. Philip E Auerswald, Lewis Branscomb, Todd La Porte, and Erwann Michel-Kerjan, xxii, 554 p. Cambridge ; New York: Cambridge University Press.

Auerswald, Philip, Lewis Branscomb, Todd LaPorte, and Erwann Michel-Kerjan. 2006. *Seeds of Disaster, Roots of Response : How Private Action Can Reduce Public Vulnerability*. Cambridge ; New York: Cambridge University Press.

Aviram, Amitai. 2005. Network Responses to Network Threats: The Evolution into Private Cyber-Security Associations. In *The Law and Economics of Cybersecurity*, ed. Mark Grady and Francesco Parisi, 143-192. Cambridge University Press, November 28.

Axtell, Robert. 2000. Why Agents? On the Varied Motives for Agent Computing in the Social Sciences. In *Proceedings of the Workshop on Agent Simulation: Applications, Models, and Tools*, ed. C. M Macal and D. Sallach, 3-24. Chicago: Argonne National Laboratory.

Baer, W. S, and A. Parkinson. 2007. Cyberinsurance in IT Security Management. *Security & Privacy, IEEE* 5, no. 3: 50-56.

Baker, Wade, Alex Hutton, David Hylender, and Christopher Novak. 2009. *2009 Data Breach Investigations Report*. Verizon Business RISK, April 15. http://newscenter.verizon.com/press-releases/verizon/2009/verizon-business-2009-data.html.

Barabasi, Alberto-Laszlo. 2003. Scale-Free Networks. *Scientific American* 288, no. 288: 9.

Bier, V., and A. Gupta. 2005. *Myopic Agents and Interdependent Security Risks. A Comment on 'Interdependent Security' by Kunreuther and Heal*. CREATE.

Boehme, Rainer, and Tyler Moore. 2009. The Iterated Weakest Link: A Model of Adative Security Investment. In , 29. London, My 19.

Boehme, Rainer, and Galina Schwartz. 2010. Modeling Cybe-Insurance: Towards a Unifying Framework. In , 36. Harvard, May 21.

Böhme, Rainer, and Gaurav Kataria. 2006. *Models and Measures for Correlation in Cyber-Insurance*. Workshop on the Economics of Information Security, June.

Bolot, Jean, and Marc Lelarge. 2008. Cyber Insurance as an Incentive for Internet Security. In *Managing information risk and the economics of security*, ed. M. Eric Johnson, 269-290. New York: Springer.

Branscomb, Lewis. 2006. A Nation Forewarned: Vulnerability of Critical Infrastructure. In *Seeds of disaster, roots of response : how private action can reduce public vulnerability*, ed. Philip E Auerswald, Lewis Branscomb, Todd La Porte, and Erwann Michel-Kerjan, xxii, 554 p. Cambridge ; New York: Cambridge University Press.

Branscomb, Lewis, and Erwann Michel-Kerjan. 2006. Public-Private Collaboration on a National and International Scale. In *Seeds of disaster, roots of response : how private action can reduce public vulnerability*, ed. Philip E Auerswald, Lewis Branscomb, Todd La Porte, and Erwann Michel-Kerjan, xxii, 554 p. Cambridge ; New York: Cambridge University Press.

Brown, Kathi. 2006. *Critical Path*. Fairfax, Virginia: Spectrum Publishing Group.

Buchanan, James M. 1965. An Economic Theory of Clubs. *Economica* 32, no. 125. New Series (February): 1-14.

Burt, Ronald S. 2005. *Brokerage and Closure: An Introduction to Social Capital*. Oxford: Oxford University Press.

Buzan, Barry. 1991. *People, states, and fear: The national security problem in international relations*. 2nd ed. Boulder: Lynne Rienner.

Buzan, Barry, Ole Wver, Jaap De Wilde, and Ole Waever. 1997. *Security: A New Framework for Analysis*. Lynne Rienner Pub, September.

Camp, L. Jean, and Catherine Wolfram. 2004. Pricing Security. In *Economics of information security*, ed. L. Jean Camp and Stephen Lewis, xv, 293 p. Boston: Kluwer Academic Publishers.

Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan. 2004. A model for evaluating IT security investments. *Commun. ACM* 47, no. 7: 87-92.

Coase, R. H. 1960. The Problem of Social Cost. *The Journal of Law and Economics* 3, no. 1: 1.

Coleman, James. 1988. Social Capital in the Creation of Human Capital. *The American Journal of Sociology* 94: S95-S120.

Davenport, Thomas H, and Lawrence Prusak. 2000. Working knowledge: how organizations manage what they know. *Ubiquity* 1, no. 24: 2.

Denning, Dorothy. 2001. Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for Influencing Foreign Policy. In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla, pgs 239-288. Santa Monica, Ca: Rand.

DHS. 2006. *National Infrastructure Protection Plan*. Department of Homeland Security.

———. 2010a. Cyber Storm: Securing Cyber Space. http://www.dhs.gov/files/training/gc_1204738275985.shtm.

———. 2010b. *Information Sharing Subgroup Meeting*. Meeting Minutes. 8.

DOE. 2007. Energy Sector-Specific Plan. Department of Energy, Office of Electricity Delivery and Energy Reliability, May.

———. 2009. *Annual Report 2008*. Energy Sector Control Systems Working Group, May.

Dunn-Cavelty, Myriam, and Manuel Suter. 2009. Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection* 2, no. 4 (December): 179-187. doi:10.1016/j.ijcip.2009.08.006.

EEI. 2009. Data & Analysis. Corporate. *Edison Electric Institute*. http://www.eei.org/whatwedo/DataAnalysis/Pages/default.aspx.

Energetics Inc. 2006. *Roadmap to Secure Control Systems in the Energy Sector*. Roadmap. Department of Energy.

EOP. 2003. *Homeland Security Presidential Directive 7*. Office of the Press Secretary.

Executive Office of the President. 2009. Energy & Environment | The White House. *the White House*. March 19. http://www.whitehouse.gov/issues/energy-and-environment.

Fahrenkrug, David. 2010. Discussion with the Director of the Air Force Chief of Staff's Strategic Studies GroupPersonal interview. May 10.

Farahmand, Fariborz, Shamkant Navathe, Gunther Sharp, and Philip Enslow. 2004. Evaluating Damages Caused by Information Systems and Security Incidents. In *Economics of information security*, ed. L. Jean Camp and Stephen Lewis, xv, 293 p. Boston: Kluwer Academic Publishers.

FBI. 2009. About InfraGard. *InfraGard - Public Private Partnership -Federal Bureau of Investigation*. http://www.infragard.net/about.php?mn=1&sm=1-0.

Gal-Or, Esther, and Anindya Ghose. 2004. The Economic Consequences of Sharing Security Information. In *Economics of information security*, ed. L. Jean Camp and Stephen Lewis, xv, 293 p. Boston: Kluwer Academic Publishers.

Garcia, Alfred, and Barry Horowitz. 2007. The potential for underinvestment in internet security: implications for regulatory policy. *Journal of Regulatory Economics* 31, no. 1: 37-55.

Gibson, William. 2004. *Neuromancer*. 20th ed. Ace Hardcover, November 2.

Goodman, Seymour, and Herbert Lin. 2007. *Toward a Safer and More Secure Cyberspace*. Washington, DC: National Academies Press.

Gordon, Lawrence, and Martin Loeb. 2004. The Economics of Security Investment. In *Economics of information security*, ed. L. Jean Camp and Stephen Lewis, xv, 293 p. Boston: Kluwer Academic Publishers.

——. 2006. *Managing Cybersecurity Resources: A Cost-benefit Analysis*. McGraw-Hill.

Gorman. 2009. Electricity Grid in U.S. Penetrated By Spies. *Wall Street Journal*, April 8, on-line edition, sec. Technology.

Gorman, August Cole, and Yochi Dreazen. 2009. Computer Spies Breach Fighter-Jet Project. *Wall Street Journal*, 4, on-line edition, sec. Technology.

Gorman, Sean P. 2006. A Cyber Threat to National Security? In *Seeds of disaster, roots of response : how private action can reduce public vulnerability*, ed. Philip E Auerswald, Lewis Branscomb, Todd La Porte, and Erwann Michel-Kerjan, xxii, 554 p. Cambridge ; New York: Cambridge University Press.

Granovetter, Mark. 1983. The Strength of Weak Ties: A Network Theory Revisited. *Sociological Theory* 1: 201-233.

Granovetter, Mark S. 1973. The Strength of Weak Ties. *American Journal of Sociology* 78, no. 6: 1360.

Gunningham, Neil, and Joseph Rees. 1997. Industry Self-Regulation: An Institutional Perspective. *Law & Policy* 19, no. 4: 363-414.

Gupta, Anil K, and Lawrence J Lad. 1983a. Industry Self-Regulation: An Economic, Organizational, and Political Analysis. *The Academy of Management Review* 8, no. 3: 416-425.

———. 1983b. Industry Self-Regulation: An Economic, Organizational, and Political Analysis. *The Academy of Management Review* 8, no. 3: 416-425.

Haimes, Yacov, and Chittester, Clyde. 2005. A Roadmap for Quantifying the Efficacy of Risk Management of Information Security and Interdependent SCADA Systems. *Journal of Homeland Security and Emergency Management* 2, no. 2 (June 14). doi:10.2202/1547-7355.1117. http://www.bepress.com/jhsem/vol2/iss2/12.

Hare, Forrest. 2009. Private Sector Contributions to National Cyber Security: A Preliminary Analysis. *Journal of Homeland Security and Emergency Management* 6, no. 1 (January 13). doi:10.2202/1547-7355.1426. http://www.bepress.com.mutex.gmu.edu/jhsem/vol6/iss1/7.

———. 2010. The Cyber Threat to National Security: Why Can't We Agree? In *Conference on Cyber Conflict Proceedings 2010*, 211-226. Tallinn, Estonia: CCD COE Publications, June.

Harris, Shane. 2008. China's Cyber-Militia. *National Journal*, May 31. http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php.

Hathaway, Melissa. 2009. Cyberspace Policy Review. Executive Office of the President, May 29. http://www.whitehouse.gov/cyberreview/documents.

Hausken, Kjell. 2006. Income, interdependence, and substitution effects affecting incentives for security investment. *Journal of Accounting and Public Policy* 25, no. 6: 629-665.

Hayek, F. A. 1945. The use of knowledge in society. *American Economic Review* 35: 519-530.

Heal, Geoffrey, Michael Kearns, Paul Kleindorfer, and Howard Kunreuther. 2006. Interdependent Security in Interconnected Networks. In *Seeds of disaster, roots of response : how private action can reduce public vulnerability*, ed. Philip E Auerswald, Lewis Branscomb, Todd La Porte, and Erwann Michel-Kerjan, xxii, 554 p. Cambridge ; New York: Cambridge University Press.

Heal, Geoffrey, and Howard Kunreuther. 2003. *You Only Die Once: Managing Discrete Interdependent Risk.* Working Paper. NBER Working Paper Series. Cambridge, MA: National Bureau of Economic Research, July.

———. 2005. IDS Models of Airline Security. *Journal of Conflict Resolution* 49, no. 2: 201-217.

———. 2007. Modeling Interdependent Risks. *Risk Analysis* 27, no. 3: 13.

Hirshleifer, Jack. 1983. From Weakest-Link to Best-Shot: The Voluntary Provision of Public Goods. *Public Choice* 41, no. 3: 371-386.

Hunker, Jeffrey. 2002. Policy challenges in building dependability in global infrastructures. *Computers & Security* 21, no. 8: 705-711.

ICSJWG. 2009. Information Sharing Subgroup Charter. Department of Homeland Security, September. http://www.us-cert.gov/control_systems/icsjwg/index.html.

INL. 2009. National and Homeland Security. *Idaho National Laboratory*. https://inlportal.inl.gov/portal/server.pt?open=512&objID=273&parentname=CommunityPage&parentid=2&mode=2&in_hi_userid=2&cached=true.

Keast, Robyn, Myrna Mandell, Kerry Brown, and Geoffrey Woolcock. 2004. Network Structures: Working Differently and Changing Expectations. *Public Administration Review* 64, no. 3: 363-371.

King, Andrew, and Michael Lenox. 2000. Industry Self-Regulation without Sanctions: The Chemical Industry's Responsible Care Program. *The Academy of Management Journal* 43, no. 4: 698-716.

Kunreuther, Howard, and Geoffrey Heal. 2003. Interdependent Security. *Risk and Uncertainty* 26, no. 2: 18.

La Porte, T. R, and D. S Metlay. 1996a. Hazards and institutional trustworthiness: facing a deficit of trust. *Public Administration Review* 56, no. 4: 341-347.

———. 1996b. Hazards and institutional trustworthiness: facing a deficit of trust. *Public Administration Review* 56, no. 4: 341-347.

La Porte, Todd. 2006. Organizational Strategies for Complex System Resilience, Reliability, and Adaptation. In *Seeds of Disaster, Roots of Response : How Private Action Can Reduce Public Vulnerability*, ed. Philip E Auerswald, Lewis M Branscomb, Todd M La Porte, and Erwann O Michel-Kerjan, xxii, 554 p. Cambridge ; New York: Cambridge University Press.

Lachow, Irving. 2009. Cyber Terrorism: Menace or Myth? In *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, 434-467. 1st ed. Potomac Books Inc., April 30.

Landwehr, Carl. 2004. Improving Information Flow in the Information Security Market. In *Economics of information security*, ed. L. Jean Camp and Stephen Lewis, xv, 293 p. Boston: Kluwer Academic Publishers.

Lewis, James. 2008. *Securing Cyberspace for the 44th Presidency*. Commission Findings. Washington, D.C.: Center for Strategic and International Studies, 12. http://www.csis.org/index.php?option=com_csis_pubs&task=view&id=5157.

Libicki, Martin C. 2007. *Conquest in cyberspace : national security and information warfare*. New York, NY: Cambridge University Press.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. RAND Corporation, November 25.

Lopez-Pintado, Dunia, and Duncan J. Watts. 2008. Social Influence, Binary Decisions and Collective Dynamics. *Rationality and Society* 20, no. 4 (November 1): 399-443. doi:10.1177/1043463108096787.

Markey, Edward. 2009. *GRID Act*.

Morgan, Granger, Jay Apt, Lester Lave, Marija Ilic, Marvin Sirbu, and Jon Peha. 2009. *The many meanings of "Smart Grid"*. Briefing Note. A Briefing Note from the Dept of Engineering and Public Policy. Carnegie Mellon University, July.

Nakashima, Ellen. 2009. Top Cybersecurity Official Resigns. *The Washington Post*, August 8. http://www.washingtonpost.com/wp-dyn/content/article/2009/08/07/AR2009080702805.html.

NERC. 2006a. Standard CIP-008-01 Cyber Security- Incident Reporting and Response Planning. FERC, June 1.

———. 2006b. Standard CIP-002-01 Cyber Security- Critical Cyber Asset Identification. FERC, June 1.

———. 2008. Information Sharing and Analysis Center for the Electricity Sector. Informational. August. http://www.esisac.com/.

———. 2009. About NERC. *North American Electric Reliability Home Page*. http://www.nerc.com/page.php?cid=1.

NSTB. 2005. *A Summary of Control Systems Security Standards Activities in the Energy Sector*. Sandia National Laboratories: Department of Energy Office of Electricity Delivery and Energy Reliability, October.

O'Hara, Vicky. 2008. *Defense Contractors May Be Chink in Cyber Security*. npr.org, May 4.

O'Toole, Laurence J. 1997. Treating Networks Seriously: Practical and Research-Based Agendas in Public Administration. *Public Administration Review* 57, no. 1 (February): 45-52.

Olson, Mancur. 1971a. *The logic of collective action; public goods and the theory of groups*. Harvard economic studies, v. 124. Cambridge, Mass.,: Harvard University Press.

———. 1971b. *The logic of collective action; public goods and the theory of groups*. Harvard economic studies, v. 124. Cambridge, Mass.,: Harvard University Press.

Olson, Mancur, and Richard Zeckhauser. 1966. An Economic Theory of Alliances. *The Review of Economics and Statistics* 48, no. 3 (August): 266-279.

Ostrom, Elinor. 1990. *Governing the Commons: The Evolution of Institutions for Collective Action*. New York, N.Y.: Cambridge University Press.

———. 1998. A Behavioral Approach to the Rational Choice Theory of Collective Action: Presidential Address, American Political Science Association, 1997. *The American Political Science Review* 92, no. 1 (March): 1-22.

Podolny, Joel M., and Karen L. Page. 1998. NETWORK FORMS OF ORGANIZATION. *Annual Review of Sociology* 24, no. 1 (8): 57-76. doi:10.1146/annurev.soc.24.1.57.

Powell, Walter W. 2003. Neither market nor hierarchy:network forms of organizations. In *The sociology of organizations*, ed. Michael Jeremy Handel, 15. SAGE.

Prieto, Daniel. 2006. Information Sharing with the Private Sector. In *Seeds of disaster, roots of response : how private action can reduce public vulnerability*, ed. Philip E Auerswald, Lewis Branscomb, Todd La Porte, and Erwann Michel-Kerjan, xxii, 554 p. Cambridge ; New York: Cambridge University Press.

Rakaczky, Ernest. 2010. Personal Interview with Invensys Control Systems Expert. April 10.

Rattray, Gregory. 2001. *Strategic Warfare in Cyberspace*. Cambridge, Mass.: MIT Press.

Roxey, Tim. 2010. Personal CommunicationE-mail. 7.

Schelling, Thomas C. 1960. *The strategy of conflict*. Cambridge,: Harvard University Press.

———. 1978. *Micromotives and macrobehavior*. New. New York: Norton.

———. 2006. *Micromotives and macrobehavior*. [New. New York: Norton.

Schelling, Thomas C. 1973. Hockey Helmets, Concealed Weapons, and Daylight Saving: A Study of Binary Choices with Externalities. *The Journal of Conflict Resolution* 17, no. 3 (September): 381-428.

Schneier, Bruce. 2003. *Beyond Fear: thinking sensibly about security in an uncertain world*. New York: Copernicus Books.

Sheffi, Yosef. 2005. *The Resilient Enterprise : Overcoming Vulnerability for Competitive Advantage*. Cambridge, Mass.: MIT Press.

Spreitzer, Gretchen. 1995. Psychological empowerment in the workplace: Dimensions, measurement, and validation. *Academy of Management Journal* 38, no. 5: 1442.

Sundelius, Bengt. 1983. Coping with structural security threats. In *Small States in Europe and Dependence*, ed. Otmar Hoell. Wien: Austrian Institute for International Affairs.

Thacher, David. 2004. Interorganizational Partnerships as Inchoate Hierarchies: A Case Study of the Community Security Initiative. *Administration & Society, 2004, 36, 1, Mar, 91-127.*

The White House. 1998. *Critical Infrastructure Protection*. Presidential Decision Directive/NSC. Washington, D.C., May 22.

———. 2008. *Comprehensive National Cybersecurity Initiative*. National Security Presidential Directive. Washington, D.C., January 8.

Thomas, Timothy. 2005. *Cyber Silhouettes*. 1st ed. Fort Leavenworth: Foreign Military Studies Office.

US-CERT. 2007. *Third Annual GFIRST Conference*. Vol. 2007.

———. 2009a. US-CERT: Control Systems. US Government. *United States Computer Incident Emergency Readiness Team*. http://www.us-cert.gov/control_systems/.

———. 2009b. Strategy for Securing Control Systems. Department of Homeland Security, October. www.us-cert.gov/control_systems/.../Strategy%20for%20Securing%20Control%20Systems.pdf.

Varian, Hal R. 2004. System Reliability and Free Riding. In *Economics of Information Security*, ed. L. Jean Camp and Stephen Lewis, 12:1-15. Advances in Information Security. Springer US.

Vijayan, Jakimura. 2009. Smart Grid vulnerabilities could cause widespread disruptions. *InfoWorld*, September 30.

Wasserman, Stanley, and Katherine Faust. 1994. *Social Network Analysis : Methods and Applications*. Structural analysis in the social sciences ; 8. Cambridge ; New York: Cambridge University Press.

Watts, Duncan J. 1999. *Small worlds : the dynamics of networks between order and randomness*. Princeton studies in complexity. Princeton, N.J.: Princeton University Press.

Wilson, Clay. 2004. *Information Warfare and Cyberwar*. Congressional Research Service, The Library of Congress.

Wilson, James. 1989. *Bureaucracy : what government agencies do and why they do it*. New York: Basic Books.

———. 1991. *Bureaucracy: What Government Agencies Do And Why They Do It*. Basic Books, January 30.

Wolfers, Arnold. 1952. "National Security" as an Ambiguous Symbol. *Political Science Quarterly* 67, no. 4 (December): 481-502.

Wu, Chris. 2006. An Overview of the Research and Development of Information Warfare in China. In *Cyberwar, netwar, and the revolution in military affairs*, ed. Edward F Halpin, Philippa Trevorrow, David Webb, and Steve Wright. New York: Palgrave Macmillan.

Wulf, William. 2007. A Perspective on the State of Cyersecurity Research in the U.S. presented at the Risk Assessment, November 6, University of Virginia.

Yin, Robert. 2003. *Case Study Research : Design and Methods*. 3rd ed. Applied social research methods series ; v. 5. Thousand Oaks, Calif.: Sage Publications.

Zaheer, Akbar, and N. Venkatraman. 1995. Relational Governance as an Interorganizational Strategy: An Empirical Test of the Role of Trust in Economic Exchange. *Strategic Management Journal* 16, no. 5: 373-392.

Zhuang, J., and V. Bier. 2006. *Subsidized Security and Stability of Equilibrium Solutions in an N-Player Game with Errors*. CREATE.

CURRICULUM VITAE

Forrest Hare is a Lieutenant Colonel in the United States assigned to the Office of the Secretary of Defense, United States Defense Department. In his most recent assignment, he was responsible for developing the United States Air Force's cyberspace strategy as part of Military Strategy for Cyberspace Operations. In addition, he has served in numerous information operations and intelligence positions world-wide.

Lt Col Hare has instructed Economics and Geography at the United States Air Force Academy and the University of Maryland Asian Division. He received his Bachelor of Science degree from the United States Air Force Academy in 1990, and a Master of Arts from the University of Illinois in 1993. He also conducted post-graduate studies at the University of Fribourg, Switzerland, under a Swiss University Grant.