SAND2011-3772C

The Economics of National Security Foresight

Drake E. Warren

Strategic Studies Department
Sandia National Laboratories
Albuquerque, NM
dewarre@sandia.gov

Prepared for Presentation at
Western Economic Association International
86th Annual Conference
San Diego, California
June 29-July 3, 2011

1 INTRODUCTION

Individuals and organizations are impacted by future events and need to make decisions with an eye to the future. There is a need to understand the future. Ideally, we would have ability to predict the future—to have "perfect foresight" in economics jargon. But perfect foresight is impossible, and even understanding uncertainty is difficult. Furthermore, even if perfect foresight were attainable, making decisions about the future is difficult in organizations because of individual preferences, such as individuals' discount rates.

This paper examines the economics of foresight. There is a limited amount of existing economics research that explicitly looks at foresight (see, for example, Coddington, 1982, who contrasts Keynes' views about uncertainty with foresight). The large amount of research on uncertainty in economics is certainty applicable to foresight, since foresight is ultimately a problem of dealing with uncertainty. I will argue that most of economics is useful for conducting foresight since the discipline is ultimately concerned with decision making, as is foresight. Economics provides ways of thinking about the future and provides lessons for the foresight practitioner.

This paper has two focuses. First, I look at how foresight can be applied to national security organizations by contrasting these organizations with firms economically. National security organizations, as with any organization providing public goods, has a responsibility to be more complete in foresight than a profit-maximizing firm because it must reflect the risk aversion of society. However, national security organizations may have fewer incentives to engage in foresight than firms. Second, I argue that a goal of foresight should be to increase resilience to future shocks. I review an existing resilience framework that has been used in homeland security applications and illustrate how that framework can provide a structured way for national security organizations to think about foresight in a way that is compatible with economic theory.

The remainder of this introduction discusses a definition of national security that will be loosely followed throughout this paper. Section 2 provides an extended discussion of the definition of foresight and how foresight can be conducted. Section 3 identifies how national security organizations are economically different than most firms, and how this impacts their abilities and incentives to engage in foresight. Section 4 focuses on resilience as the goal of foresight. Section 5 concludes.

1.1 What is National Security?

This paper talks specifically about national security organizations, but does not prescribe precisely what national security organizations are.

A report by the Princeton Project on National Security (Bergen and Garrett, 2006) reviews many definitions of national security. It finds that the traditional views of national security "have focused almost exclusively on the potential of violent attack by other countries on the United States, its citizens, and its vital overseas interests," a view they term the "violence paradigm" (p. 1). More expansive views of national security include transnational threats such as "terrorism, environmental degradation, and the spread of infectious diseases" and may include concepts such as "human security" and "ecological security" (p. 4). The report concludes that underlying all of these views of national security is that "national security policy operates to secure primary public goods that are at the heart of the social contract between the people and its government" (p. 2).

This paper's discussion of national security organizations will focus on those organizations that engage in military, intelligence, and diplomacy activities (e.g., the U.S. Department of Defense, the intelligence community, the U.S. Department of State, and other organizations that support these activities.) This discussion is flexible and can be applied to any organization that secures public goods, thus it is flexible to a variety of definitions of national security and functions of government.

2 WHAT IS FORESIGHT?

Random House Dictionary's definitions of foresight summarize it well. The dictionary's first definition is "care of provision for the future; provident care; prudence," while its fourth definition is "knowledge or insight gained by or as by looking forward; a view of the future," (Random House, 2011). These definitions emphasize that foresight is insight or knowledge, but also emphasizes that foresight requires that the insight or knowledge be used to guide future actions. These future actions make prudent decisions based on this foresight information. Thus the discipline of economics, with its focus on making prudent decisions to improve the future, is a type of foresight.

Foresight is not the same thing as forecasting or predicting, but forecasts and predictions may be an element or a tool of foresight if they can be used to produce "knowledge or insight" that can acted upon to improve some future. Foresight emphasizes the development of insights that apply to the big picture, thus foresight is similar to applied wisdom.

The national security community often takes a particular view of foresight that is echoed in the Project on National Security Reform's definition of foresight as "the ability to anticipate unwelcome contingencies" (p. vii). This definition seems to assume that the primary function of national security to predict bad things that will happen, and secondarily, once the future has been correctly predicted, national security should do something to prevent the bad thing from occurring. Furthermore, the definition assumes that the focus of national security foresight should be looking for problems, but this discounts that anticipating *opportunities* can sometimes be as important to engaging in effective foresight as anticipating problems. Unfortunately, missing a problem is more obvious and may result in greater personal, organization, and political cost than missing an opportunity.

To create effective organizations in the long-run, decision makers in all domains must engage in foresight. All domains must also use resources effectively in the near-term so that the organization can thrive and continue exist in the future. Resource tradeoffs between the short term and long term involve investment or savings decisions.

National security organizations and firms share similar views and terminology about the hierarchy of goals, actions, and decision making. There are three commonly accepted levels at which organizations act: the strategic level, the operations level, and the tactical level.

Strategic Level: The strategic level is the highest level in both national security and business domains. The U.S. military's *Doctrine for Joint Operations* states that the strategic level of war is "that level of war at which a nation… determines national or multinational strategic security objectives and guidance and develops or uses national resources to accomplish these objectives" (Joint Chiefs of Staff, 2001, p. II-2.) When applied to the business domain, the strategic level includes "decisions with long-term effects, such as investments in machinery or expansion" (Gustavsson, 1984, p. 803.) In logistics networks, for example, the strategic level involves "prescribing facility locations, production technologies and plant capacities" (Schmidt and Wilhelm, 2000, p. 1504).

Operational Level/Tactical Level: The operational level is the middle level in national security while the tactical level is commonly the middle level in business domains. The operational level of war "links the tactical employment of forces to strategic objectives. The focus at this level is on operational art—the use of military forces to achieve strategic goals through the design, organization, integration, and conduct of strategies, campaigns, major operations, and battles" (Joint Chiefs of Staff, 2001, p. II-2.) In the business domain, the tactical level deals with problems in the "medium-term, such as changes in design or rate of production" (Gustavsson, 1984, p. 803.) In logistics networks, for example, "the tactical level prescribes material flow management policy, including production levels at all plants, assembly policy, inventory levels and lot sizes" (Schmidt and Wilhelm, 2000, p. 1511).

Tactical Level/Operational Level: The tactical level in national security is the lowest level while the operational level is the lowest level in business domains. The tactical level of war "is the employment of units in combat. It includes the ordered arrangement and maneuver of units" in engagements and battles (Joint Chiefs of Staff, 2001, p. II-3.) In the business domain, the operational level deals with "short-term" problems like "having to replan in order to cope with a breakdown of vital machinery, or an unexpected shortage of material" (Gustavsson, 1984, p. 803.) In logistics networks, for example, "The operational level schedules operations to assure in-time delivery of final products to customers" (Schmidt and Wilhelm, 2000, p. 1514).

In national security, these levels can apply beyond the levels of war. For example, Vego (2009, pp. VIII-25 – VIII-43) applies the levels to strategic intelligence, operational intelligence, and tactical intelligence. Many national security activities are similar to business areas, like logistics chains in the military and arms systems production, which further increases the similarities between national security and firms.

These levels are continuous and cannot be delineated precisely. For example, the Air and Space Power Mentoring Guide (U.S. Air Force College of Aerospace Doctrine, Research and Education, 1997) says that "The boundaries of the levels of war and conflict tend to blur and do not necessarily correspond to levels of command." However, responsibilities for each level tend to follow military hierarchies and scope. "[T]he strategic level is usually the concern of the National Command Authorities (NCA) and the highest military commanders, the operational level is usually the concern of theater commands, and the tactical level is usually the focus of subtheater commands." Firms are likely to have a similar hierarchy where strategy is the principle responsibility of executives and operations and tactics flow down to lower levels of management.

For simplification and to reduce confusion, I will combine the tactical and operational levels and refer to them as "operational." This operational level tends to operate in the shorter term and be concerned with immediate challenges, so, foresight activities are usually aimed at informing strategy. For example, strategic planning activities are a natural target for combining with foresight activities because they enable foresight to be integrated with an organization's long-term planning.

There may be a tendency for leaders to exclusively apply foresight to strategy. This is a mistake because challenges and opportunities emerge at both the operational and strategic level. A prime example of this is homeland security incidents, such as natural disasters and terrorist events, which can interrupt organization's operations, thereby threatening their strategic goals. An organization with foresight might implement strategies to make its operations more resilient to these events. Section 4 expands on resilience in much greater detail.

Because strategy and operations are intertwined, there is a danger to organizations that stovepipe operational domains. Problems and opportunities cross between operational boundaries and the boundary between operations and strategy. If operational foresight in individual stovepipes ignores the other operational stovepipes, or if strategic foresight ignores operational foresight, there is a danger of making poor decisions. Unintended consequences would be more likely in such a situation. An important principle of systems engineering called the principle of suboptimization should sound familiar to economists. The principle "states that optimization of each subsystem independently will not in general lead to a system optimum and, more strongly, that improvement of a particular subsystem may actually worsen the overall system" (Machol, 1965, p. 1-8), similar to an economy that violates the assumptions of perfect competition.

Although the link between foresight and strategy seems most obvious, economics and economists probably have the greatest impact on operational foresight. Because operational issues tend to be in the present, there are usually data to support quantitative economic methods. Uncertainty tends to be low and can often be quantified, making operational issues more compatible with models of the optimization-based neoclassical economics paradigm.

Economics also impacts many strategic foresight issues, but the link here is not as strong. Certainly economic theory produces strategic policy insights, but the exposition tends to shift from the quantitative language of mathematics and statistics to qualitative models and persuasion. Compare, for example, Milton Friedman's and Paul Krugman's academic and policy work. Game theory is a quantitative tool that has had success at applying to both operational and strategic problems, but many of the other economic methods that have been used, like evolutionary economics, tend to be more qualitative in nature. The asymmetry of available data about the past and the future certainly make econometric methods more difficult to apply to the future, especially to futures that change in fundamental ways, which is where foresight is needed most. Econometric forecasting models have some value in foresight, but usually to the short term when the structure of an economy remains similar to the past, from which the model was estimated.

Traditional non-economic foresight methods also tend to be qualitative as well, and focus on communications. Scenario methods are a common qualitative method that develop and analyze alternate future scenarios as a way of evaluating important future drivers and evaluating levers to affect those drivers. The National Intelligence Council's Global Trends project (see National Intelligence Council, 2008, for the latest report) uses scenarios (along with collaboration with a wide variety of researchers and policymakers from around the world) to identify key trends that will affect the world (and organizations' strategy and operations) over the next 15 years. An early foresight method was the Delphi Technique, which provided a systematic methodology to "obtain the relevant intuitive insights of experts and then use their judgments as systemically as possible" (Helmer, 1967). The Delphi Technique recognized that "projections into the future… are largely based on the personal expectations of individuals rather than on predictions derived from a well-established theory," a situation that arises because "[t]he traditional methods of the social sciences are proving inadequate to the task of dealing effectively with the ever-growing complexity of forecasting the consequences of alternative policies" (pp. 3-4). The Delphi Technique provided a way of stimulating various experts to interact and learn from each other.

One major disadvantage of traditional foresight methods like scenarios (in many communities) is that they tend to be qualitative and appear relatively less rigorous than quantitative methodologies. That is, they do not speak the language of science; they value skills like creativity and imagination rather than rigor. However, a greater diversity of skills in the development of foresight is likely to

produce stronger results that are more actionable. The rigor of foresight increases with increased participation in foresight. Furthermore, as computing power has increased over time, simulation methods such as systems dynamics and agent-based models have become more common and have helped facilitate foresight and lent more credence to the results of foresight by framing it in the quantitative language of traditional science. A possible danger of these simulation methods is that they may be guilty of "cargo cult science" if used improperly. The simulation methods look like science, but if the assumptions that run the model lack rigor, it may be a case of garbage in, garbage out that fools people into believing the results are rigorous and scientific. Perhaps it is this danger that has made the field of economics reluctant to embrace many of these new methodologies. Reaching the same levels of rigor in foresight as in hindsight will never be possible because of the uncertain nature of the future, but—if kept in proper perspective—simulation modeling may aid in thinking about the future and improve foresight.

3 HOW ARE NATIONAL SECURITY ORGANIZATIONS DIFFERENT ECONOMICALLY THAN PROFIT-MAXIMIZING FIRMS?

As the previous section illustrated, national security organizations and firms engaged in business activities have many similarities in how they make decisions strategically and operationally. Foresight aids either type of organization in making both types of decisions.

This section discusses several important ways in which national security organizations in the United States differ from typical, profit-maximizing firms. These ways generally make the production of foresight more difficult.

3.1 Profit Maximization vs. Welfare Maximization

The explicit goal of firm is to maximize profits in order to maximize returns to the owner. This goal is very straightforward, although it is difficult and complex to achieve over time. There are clear metrics available to measure progress towards this goal (profit is revenue minus costs; accountancy provides standard methods for estimating these metrics over time).

National security organizations do not have such an explicit goal. The explicit purpose of each organization varies, but in a larger sense all the purposes are to maximize public welfare. The difficulties and controversies in maximizing welfare are well-known. The term "welfare maximization" is itself a misnomer because any world beyond a contrived model will have no universally agreed level of maximized welfare. The difficulties of maximizing welfare (or merely increasing it) are furthered by the political system, which ultimately decides whose welfare is being maximized and what explicit goals the national security system needs to achieve to increase welfare.

Public choice theory has highlighted many of the difficulties in government that lead to inefficient and ineffective production of government services, and may be applicable to national security organizations, which are either run or funded by governments. Many military programs, for example, have been criticized as wasteful spending.

Economists have often offered principles from market economies to guide national security decisions. For example, Hartley (1997) suggests that several market solutions should guide the armed forces and the defense industries. The provision of national security could be guided by

market principles, but the fact remains that national security is a public good ultimately supplied by monopolist/monopsonist organizations that are not subject to true market forces, as would a typical private firm. On top of these difficulties, the provision of national security is subject to an often politicized environment where the goals of policymakers and bureaucrats may diverge from the goals of welfare maximization. All of these problems may be reduced by applying market principles and by attempting to provide good governance, but these challenges ultimately mean that national security production is likely to always suffer from a higher degree of inefficiency than market production.

3.2 Incentives for Long-Term, Strategic Thinking

Decisions in firms are typically made by entrepreneurs or managers guided by boards of directors who are typically assumed to be managing the long-term profit flow of the firm. In reality, issues of agency and incentives mean that this model of the firm is an ideal rather than the actual behavior of a firm (the next section discusses some of these issues in more detail). For example, many business leaders think that the incentives for short-term profit are making it difficult to pursue long-term growth and sustainable profits (Aspen Institute Business and Society Program, 2009). Poterba and Summers (1995) found evidence of this "short-termism" in CEO's discount rates, which averaged 12.2 percent in a survey—much higher than the cost of capital. Corporate-wide foresight is often not priority of management. Hamel and Prahalad (1994, p. 4) argue that only 2.4 percent of senior executive time is spent looking at future corporate issue (they contend that rest of the time is spent looking at current issues or narrow issues that affect only the executive's line of responsibility.)

National security organizations include firms as well as the politicians who guide national security policy and the military and civil service who help execute it. Politicians are usually considered to have few incentives to promote long-term policies since their most immediate concern is the next election. For example, Nordhaus (1975) finds evidence that politicians support economic policies that have an aim of improving election chances and result in a "political business cycle." The focus on the short term is often lamented by policymakers in the national security community. For example, a former DoD comptroller blames U.S. failures in Afghanistan on "the American predilection to focus on the here-and-now" and the focus of "American policymakers of both parties… on the immediate, the must-do; they devote little time to considering the long-term consequences of their short-term policies or creating mechanisms for dealing with them" (Zakheim, 2011).

The U.S. military is a meritocratic institution. Officers may hope to have a long career in which they advance up the ranks, thus they have incentives to engage in longer-term thinking. The nature of military acquisition, in which systems take many years to develop and remain in service into the distant future when the nature of threats and adversaries is highly uncertain, encourages long-term thinking. On the other hand, most assignments last for a relatively short period, which may make longer-term thinking more difficult. However, the nature of these assignments, which since the passage of the Nichols-Goldwater act in 1986 have also encouraged cross-service Joint Duty Assignments, encourages a more holistic view that may produce more effective foresight by working across stovepipes.

Bureaucrats are often stereotyped as unmotivated shirkers. The motivation behind this stereotype is probably motivated in part by the insulation of much of the civil service from features of the private labor market such as pay for performance and job insecurity. The National Committee on Public

Service concluded that the civil service was characterized as a system where "the best are underpaid; the worst overpaid" where "the untalented stay too long" (National Committee on Public Service, 2003, p. 1). There have been occasional attempts at reform, such as the Civil Service Reform Act of 1978 that attempted to increase civil service incentives by introducing merit pay for some positions, such as upper-level managers. Some agencies, like the Department of Homeland Security (DHS) and Department of Defense (DoD), have looked at eliminating automatic annual pay increases (see Ingraham, 2006). This line of reasoning is appealing to economists, whose models of behavior are motivated by self-interest, of which monetary incentives are an easy to measure proxy. Nevertheless, monetary incentives are not the only source of motivation, as is demonstrated in much of the literature about compensating differentials. Prendergast (2007), for example, creates a model where civil service employees have an intrinsic motivation in their work (civil servants care about social welfare) and shows how such a motivation may lead to more efficient outcomes.

Perhaps a bigger cause of difficulties in the civil service is structural. Unlike the private sector, with its relatively simple problem of profit maximization, the civil service is charged with the complex problem of executing policies that maximize welfare. Many of the jobs in the civil service, especially high-level managerial positions where foresight would most often be executed, the work of the civil service is not comparable to the work of the private sector which makes marking pay to the labor market difficult (National Committee on Public Service, p. 9) and increases the challenges in job execution. Additionally, bureaucracy may be hampered by "a maze of rules and regulations" that makes the civil service much less effective (National Committee on Public Service, p. 1). Furthermore, the civil service operates within a very hierarchical bureaucracy whose effectiveness as a whole may be hampered by barriers to working between agencies that create both operational and strategic stovepipes. For example, the Project on National Security Reform characterizes U.S. national security as being paralyzed by "parochial departmental and agency interests" (Bergen and Garrett, 2006, p. viii) suggesting that the actual goal of the civil service is to maximize agency welfare rather than national welfare. The Project recommends a number of reforms that would increase interagency cooperation within the national security bureaucracy, similar to how the Nichols-Goldwater Act incentivized joint service cooperation in the military. Some of the reforms in agencies like DHS and DoD may actually run counter to theses goals of unifying the bureaucracy by fragmenting the civil service (Thompson, 2006).

3.3 Incentivizing Opportunities

Commercial businesses, particularly entrepreneurs and entrepreneurial firms, often place a greater emphasis on anticipating future opportunities than do national security organizations. This distinction likely arises from the different incentives faced by these actors.

Entrepreneurs and firms are largely concerned about making profits. Their strategic and operational decisions can have both upside and downside risks.[1] When entrepreneurs and firms are successful,

[1] The term "risk" in this paper is used similarly to the way it is used in risk management applications, where risk is "determined by its likelihood and the associated consequences," (DHS, 2010, p. 27), i.e., likelihood multiplied by consequence. "Uncertainty" can refer to the "degree to which a calculated, estimated, or observed value may deviate from the true value" (DHS, 2010, p. 38), so it may or may not be quantifiable. "Uncertainties" refers to events or factors, which may or may not be totally unexpected (i.e., it includes unknown unknowns), that contribute to uncertainty. These definitions differ from those of Knight (1921), which are often used by economists, where risk and uncertainty are understood as synonyms for "measurable" and "immeasurable," respectively.

they profit; when they are unsuccessful, they lose money. Attempting to take advantage of opportunities is risky since there are both upside and downside risks. In cases where the upside risk of seizing an opportunity appears much larger than the downside risk, entrepreneurs and firms have a financial incentive to act.

Firms (more exactly, their owners) have limits to downside risk (the value of the firm) but no limits to the upside risk. Further, firms and their owners often have a capacity to manage multiple risks to mitigate the net downside risk. On the other hand, when the managerial and ownership functions of firms are separate (for example, when a company is publicly owned) managers do not personally face the same incentives as they would if they had they owned the firm. In such a situation, managers might be less willing to pursue opportunities. In this sense, publicly owned firms and most national security agencies have a similar externality problem, where personal costs and benefits do not align with societal costs and benefits. This externality problem is somewhat mitigated in companies because the labor market provides a mechanism for aligning the manager's incentives with the firm's costs and benefits. If a firm does well, it will better reward employees, and other employers will view the firm's success as a signal that its managers are productive, thereby pressuring wages upwards (see Fama, 1980). Success and failure in national security is much less verifiable by the labor market because measuring welfare is more difficult than measuring profit. Furthermore, national security agencies tend to be highly secretive, unlike publicly traded companies that must keep the public informed with details of their success and failure. Therefore, the labor market is unlikely to align the incentives of managers of national security organizations with welfare maximization as well as it aligns the incentives of managers of firms with profit maximization.

The secrecy of national security organizations exacerbates an asymmetry between success and failure. In many cases, when a national security organization is successful, the success will be closely held. Failures are more likely to be made public. As a basic example, a primary task of national security organizations is to keep secrets away from adversaries. Only when an organization fails at this task does it become public; success is not widely recognized. A similar example is the safety and security of nuclear weapons. A failure would be catastrophic, and success is expected. Different levels of success (i.e., measuring how well the nuclear complex has managed its risk) are impossible to measure quantitatively and difficult to measure qualitatively and subjectively by the actors within the complex itself (see Committee on Risk-Based Approaches for Security the DOE Nuclear Weapons Complex, 2011). In such a situation, the labor market has little way of ascribing a manager's contributions to success.

The asymmetry between success and failure in national security organizations means that the incentives to take advantage of opportunities are low and national security organizations are driven towards risk aversion. Risk aversion by firms is generally seen as socially undesirable since it reduces returns to shareholders who can choose how to manage risks for themselves (but it may be beneficial to firms' managers—see Amihud and Lev, 1981.) The same logic does not apply to national security organizations; national security is a public good and citizens have little capacity to manage national security risks. Therefore, risk aversion in national security organizations is likely desirable if it reflects risk aversion in society. However, this fundamental difference between profit-seeking firms and national security organizations makes effective foresight that manages both unwelcome contingencies and opportunities more difficult. Moreover, a risk-averse national security organization is likely to be less efficient and more wasteful than a risk-neutral firm.

3.4 Demand, Adversaries, and Zero Sum Games

The nature of adversaries is another aspect where firms and national security organizations differ.

In the neoclassical, perfect competition model that forms the basis of much economic modeling, firms do not really have adversaries. There are large numbers of firms, and a single firm is too small to affect other firms. Instead, each firm works through markets and takes the demand of those markets (as well as the supply of its suppliers) as exogenous. As the perfect competition assumptions are relaxed (e.g., in models of oligopoly), firms can affect each other with their decisions, but this interaction remains relatively indirect since it is ultimately the market that determines how a firm should be behave.

Even in these non-adversarial models, firms usually engage in market intelligence to understand the demand for their products, the supply of their inputs, and how demand and supply might be expected to behave in the future. Firms also engage in business intelligence to better understand their firms operations. These types of intelligence feed into a firm's strategic planning and strategic decision making, such as its investment choices.

Similar issues are important to national security organizations, with some notable differences. Most similarly, national security organizations (in fact, most government organizations) need to procure inputs (such as technology and human capital) from competitive markets. Thus market intelligence also guides these organizations' long-term strategy.

Rather than a market that determines the demand for a firm's production, policy through the budgeting process ultimately determines the funding available for national security organizations. This is a subtle, but meaningful difference since each firm's demand is usually determined by the interaction of quantities and prices determined by markets, while the demand for national security organizations is a function of overall appropriations. In this sense, the "demand" acts more like an input to the production of the national security public good than it does an output. These appropriations may be a function of quantities and costs, and costs are often difficult to measure due to the absence of markets.

Like firms, national security organizations engage in business intelligence to understand and improve their organization. For example, both the military and manufacturing industries commonly develop intelligence about their supply chains. In both firms and national security organizations, this type of business intelligence may be sensitive if the firm or organization draws an advantage from protecting its dissemination.

Moving from the operational to the strategic level, both firms and national security organizations have an ability to affect their demand curves—i.e., demand is not exogenous. The field of marketing focuses on how firms can increase demand for their products. National security organizations can affect their demand through political processes, for example, through lobbying. The political system places different constraints on different types of organizations; a government agency obviously cannot hire a lobbyist, but may be able to influence appropriators in other ways. Thus, the ways in which national security agencies influence demand are more complex.

As the next section discusses, another important goal of many national security organizations is influencing legitimacy as it is a fundamental input to power. For example, diplomacy tries to build coalitions that help build power to convince others to take beneficial actions while minimizing force.

Thus, firms' marketing and a nation's influence are similar since they ultimately impact the demand for a firm's or national security organization's outputs.

As the field of industrial organization has grown, the importance of interactions between firms has been recognized. Game theory has been used in industrial organization to model these interactions between firms. In such models, firms can act more directly as adversaries to one another. The goals of most national security organizations are to manage adversaries, for example, by defeating them or deterring them from acting in undesirable ways. Similarly to industrial organization, many analysts have modeled these interactions between adversaries with the tools of game theory. For example, Thomas Schelling, who won the 2005 Noble for "having enhanced our understanding of conflict and cooperation through game-theory analysis," did a considerable amount of work in modeling nuclear deterrence (e.g., his Nobel acceptance talk, Schelling, 2005). Therefore, to understand adversaries and competitors motivations, capabilities, and actions, both firms and national security organization often conduct research on their competitors and adversaries to help guide decisions.

As firms interact, they most often engage in non-zero sum games. Market interactions are based upon mutually beneficial arrangements, thus market competition tends to make all participants better off (provided there are no externalities). The clichés of the rising tide lifting all boats or making the economic pie larger describe how the outcome is non-zero sum results.

Some national security issues are also non-zero sum games. Much of diplomacy is about fostering relationships and agreements that make all parties better off. For example, economic diplomacy often removes barriers to trade in an effort to improve all participants' economies.

At the heart of many national security issues are zero sum issues. In the past, mercantilism led nations to war over what they believed were finite resources. More recently, ideological issues have driven conflicts. Underlying many of these zero sum games is the distribution of economic and political power, which is often thought to be finite. These zero sum games become non-zero sum if conflict is a possibility (because conflict is costly). This allows the possibility that diplomacy or deterrence will lead to equilibrium where players will be better off overall by avoiding conflict, but it creates a danger if the only way for a player to become better off is through conflict, especially if players have different perceptions over their capabilities and each other's beliefs. For example, two adversaries might believe that they would be better off if they prevailed in a conflict, and both might believe that they have good chances of prevailing in a conflict or deterring their adversary, so each may choose to fight.

Because of the importance of capabilities and beliefs, it is important for national security organization foresight to be informed by knowledge of the adversary. What does the adversary believe? What are the adversary's capabilities? It is also important to understand the limitations of this knowledge, since a misunderstanding of the adversary that leads to overconfidence in mistaken beliefs could lead to a worse outcome than if no knowledge had been discovered in the first place. Thus, a fundamental requirement of effective national security foresight is that it be resilient to a highly uncertain future. Section 4 discusses in greater detail how national security foresight may be made more resilient.

3.5 Implementation of Foresight

Firms and national security organizations have different resources available to implement foresight. National security organizations are either government organizations or private organizations

empowered by the government. The backing of government gives these organizations a large degree of control, hence national security organization operate in **control space**. For example, national security organizations are empowered with the ability to use force against other nations and nonstate actors. Weapons and systems manufacturers, which are often firms, are funded to support this use of force. Diplomacy provides a nonviolent complement to force to achieve international political goals, and can also help reach agreements (e.g., treaties and United Nations Resolutions) with the power of law.

On the other hand, most firms operate in **voluntary space**, where decisions are based upon the will of individual people or individual firms. In the voluntary space, actions are taken which are mutually beneficial to all parties who take part in agreements. Thus actions in voluntary space tend to increase overall welfare, whereas actions in the force space will often be zero-sum or be mutually damaging.

Schlesinger and Phillips (1959) identified the battle between voluntarism and control as the great ideological battle of the Cold War, and predicted that the United States would move towards greater convergence with the Soviet Union as the United States moved towards control and the Soviet Union moved towards voluntarism. Indeed, the two spaces often play adversarial roles. For example, through regulation governments compel non-voluntary actions by the private sector in an effort to improve welfare. The two spaces can also play complementary roles. The concept of "regulatory capture" describes how firms in the private sector attempt to influence regulators (in the control space) to increase their profits. For example, firms may influence regulators to restrict entrance to a market, impose anti-competitive rules, or permit externalities. Similarly, in national security, many worry about the "military-industrial complex" in which the defense industry has "misplaced power" to induce the government to engage in actions that are beneficial to the industry but not necessarily to the country (Eisenhower, 1961).

There is a third space that both affects and is affected by the previous two spheres. General Norton A. Schwartz, the Chief of Staff of the Air Force, terms this "legitimacy" (Schwartz and Kirk, 2009), i.e., **legitimacy space**. Schwartz and Kirk focus on the "economy of deterrence," which they describe as the use of legitimacy and control to deter and dissuade allies and insure and assure allies. To accomplish these goals in today's world, they argue that policymakers need to draw on both resources within both spaces, and they argue that military thinking needs to move beyond "a purely control-oriented focus to include both legitimacy and control in every case." This focus on legitimacy is international—a nation will be more powerful if it is respected by both its allies and its adversaries. The U.S. *National Security Strategy,* for example, recognizes the U.S. "moral example" as being fundamental to U.S. national security (Obama, 2010, p. 1). Domestic legitimacy is important for power, especially in a democratic country (but even in nondemocratic countries) because domestic legitimacy provides resources to build control. As a resource, organizations in the control space can both invest in legitimacy (e.g., by engaging in foreign diplomacy, foreign aid, military diplomacy, or utilizing weapons with less collateral damage) and consume legitimacy. Similarly, organizations in voluntary space, like firms, must build legitimacy (e.g., through marketing) to help increase demand for their products and can consume legitimacy if they produce poor products or act unethically. In cases where the relationship between organizations in control space and organizations in voluntary space is adversarial, both can draw on resources in legitimacy space for support.

Figure 1 diagrams this resource triad. Organizations and individuals across the globe belong to different spaces. National security organizations representing the U.S. government as well as state and local governments and organizations within foreign governments exist in control space.

Relationships between the different organizations can be cooperative or adversarial depending upon their goals. When organizations engage in foresight, they are essentially investing in resources. For example, if the U.S. Agency for International Development (USAID) provides development aid in another country, they may be investing in a combination of individuals and organizations (such as non-governmental organizations) in legitimacy space, individuals and firms within voluntary space, and government organizations in control space. One likely goal of these investments is to build influence with these investments, thus foreign aid investments are investments in national security resources.

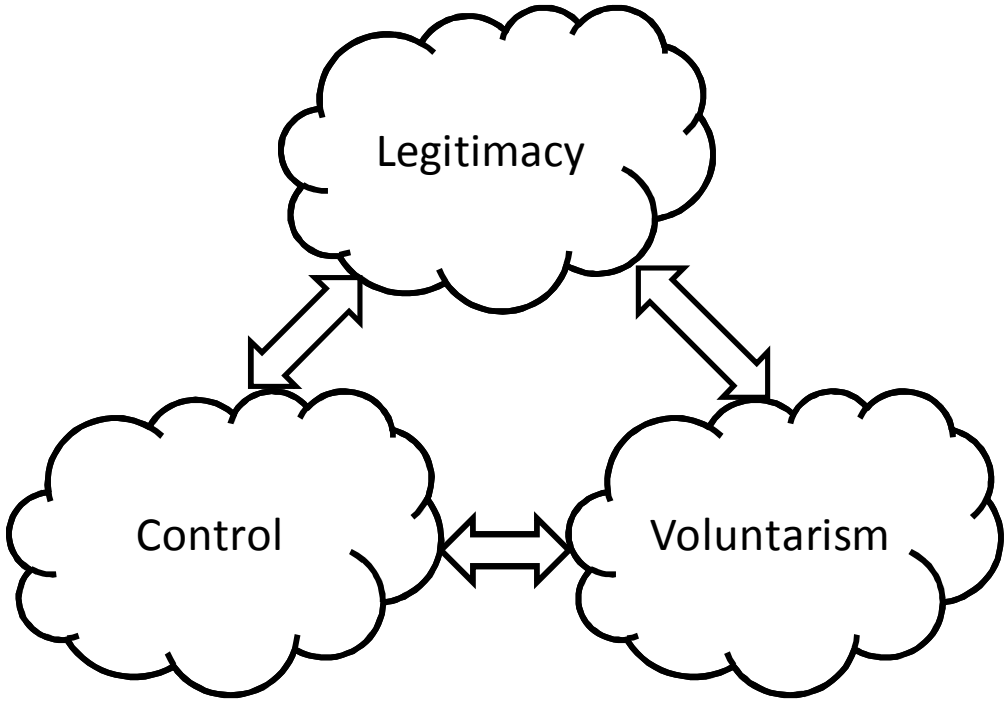

Figure 1: Triad of Resources Available to Implement Foresight

Organizations within each space can purposefully invest in organizations and resources in all the spaces, both domestically and internationally. For example, in a highly-centralized, autocratic nation, organizations in control space may have a concentration of power and have control over domestic organizations in all three spaces. In decentralized nation there may be powerful organizations in all spaces, so the ability of any one organization to influence the others will be more limited. In the former nation, there are fewer barriers to implementing foresight, but in the latter nation, foresight will likely be more robust. Just as Hayek (1945) described the knowledge problems that diminish the effectiveness of economic central planners, similar knowledge problems in national security may impact the ability of centralized national security organizations to implement national security foresight.

Koliba, Mills, and Zia (2011) construct a similar model, which they term "accountability in governance networks." Their three accountability frames describe the governance system and how it acted following Hurricane Katrina. These frames relate directly to the three previously described resources spaces: "democratic (elected representatives, citizens, and the legal system)" corresponds

to legitimacy, "market (owners and consumers)" partially corresponds to voluntarism,[2] and "administrative (bureaucratic, professional and collaborative)" corresponds to control. Koliba, et al. describe how these governance networks responded to a disaster, but the same network of resources also acts (or, perhaps in the case of Katrina, fails to act) before events to implement foresight. The next section describes a resilience framework that can be used by actors within governance networks to guide foresight so consequences are mitigated in low-probability, high-consequence events.

4 RESILIENCE AS THE GOAL OF FORESIGHT

Enhancing the resilience of the United States is a central goal of the U.S. *National Security Strategy*, which recognizes that "we will not be able to deter or prevent every single threat" (Obama, 2010, p. 18). Post-Katrina, resilience has been a growing focus of homeland security policy, particularly in regards to the resilience of society and the economy to natural hazards like hurricanes. It is clear that many hazards cannot be prevented because mankind has a very limited capacity to manage the environment. The *National Security Strategy* recognizes that malicious threats to national security and the vulnerabilities they exploit cannot be eliminated with certainty, so reducing consequences by increasing resilience is prudent to lower overall risk. In national security applications, an added benefit of resilience is that adversaries may be less likely to engage in acts with less severe consequences because it may influence the balance between those adversaries' costs and benefits.

Sandia National Laboratories has developed a resilience assessment framework that can be used to assess resilience of systems to specific threats and hazards (for a detailed description, see Vugrin, et al., 2010). This framework has been applied to many case studies focused on natural hazards (e.g., hurricanes in Vugrin, Warren, and Ehlen, 2011.) This section provides a brief overview of the Sandia resilience framework, followed by a discussion of how the framework might be extended to guide foresight in national security organizations. The section concludes by discussing justifications for regulating firms (i.e., relationship between control space and voluntary space) when the lack of resilience of firms in voluntary space may threaten national security.

4.1 Resilience Assessment Framework

According to Sandia's resilience assessment framework:

> Given the occurrence of a particular disruptive event (or set of events), the resilience of a system to that event (or events) is the ability to efficiently reduce both the magnitude and duration of the deviation from targeted system performance levels (Vugrin, et al., 2010, p. 83).

This definition is illustrative graphically and quantitatively in Figure 2 below. The figure shows the calculation of "resilience cost," which is a proxy for system resilience; a system with greater resilience will have lower resilience costs, and vice versa. Resilience is a function of two quantities, the systemic impact (SI), which measures the "magnitude and duration of the deviation" of system performance (SP) from targeted system performance (TSP), and total recovery effort (TRE), which measures how "efficiently" SI is reduced. Thus, resilience involves a fundamental tradeoff between the reduction in SI (i.e., the benefits) and the TRE required to engage in that reduction (i.e., the costs). Vugrin, et al. (2010) researched existing resilience definitions and measurement

[2] Consumers seem to fit better into legitimacy space when they consume or perform citizen duties, but fit into voluntary space when they supply labor to voluntary organizations.

methodologies and found that it is common for resilience researchers to focus on benefits, but previous research had failed to also account for costs, so this resilience framework is uniquely compatible with economic thinking.

The authors of this framework have experienced some resistance from some members of national security communities to the inclusion of resilience costs. This resistance seems motivated in two ways. First, some think that the national security community has a large enough pool of resources that the TRE does not really matter. However, resources are not truly unlimited, especially in the short term. For example, there is a finite number of trained troops or weapons systems, and it takes time to get them into position, so the resources that can be utilized are incontrovertibly scarce. Second, some think that the benefits of national security are of such high importance that they are incomparable with financial costs. However, the total recovery effort need not be measured in money, but instead in resources more generally (e.g., troops), which may be of greater comparability to national security benefits. Furthermore, the resilience cost methodology can be weighted by α to compare SI and TRE (which, more generally, can be allowed to be multidimensional to weight various measures of TRE and vary over time.) With the recent debates on the federal budget, it seems that there is a greater recognition of the importance of resource constraints, and this importance is likely to grow in the near-term.

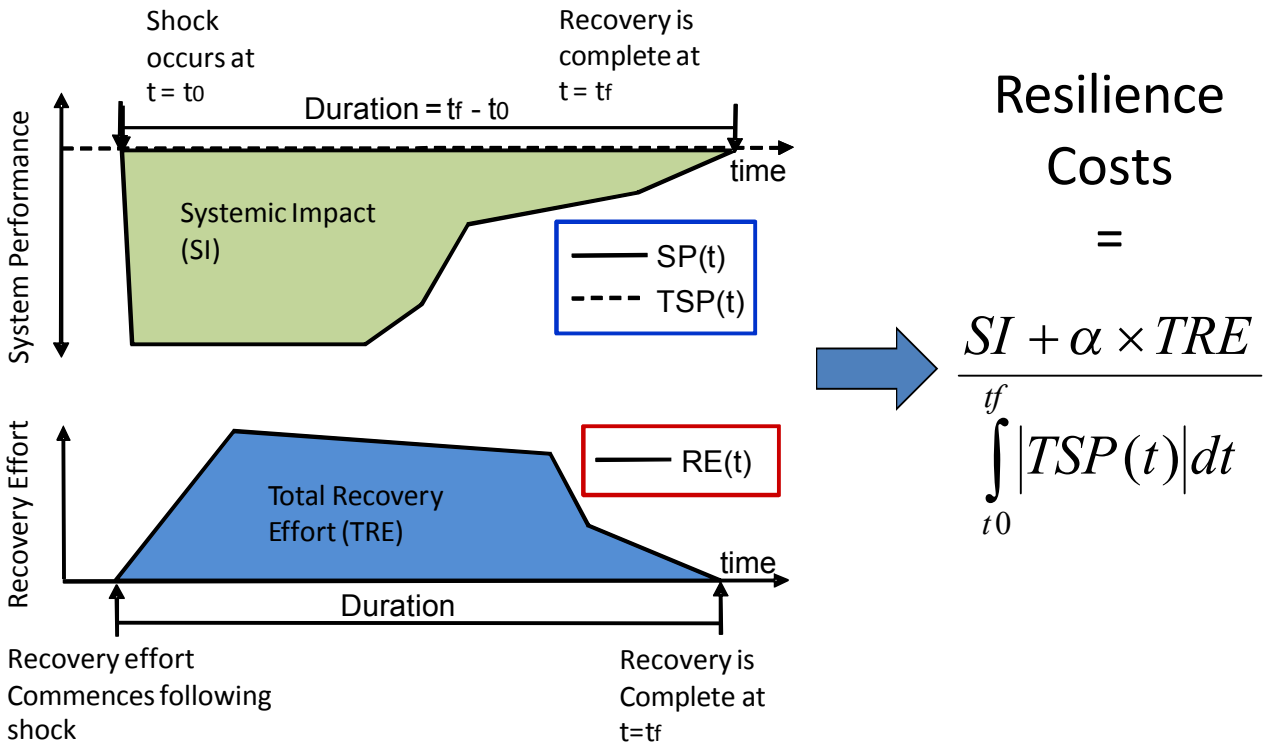

Figure 2: Illustration of Resilience Costs

Targeted system performance (TSP) is a subjective quantity that describes how a system should behave following a disruption. In applications of this framework, it has been most common to set this quantity to some measure of a system's performance before the shock occurs (e.g., the average production levels in an industry that is disrupted by a hurricane). In many national security

applications, however, TSP will not be constant. For example, the performance of the military is hoped to increase substantially following the outbreak of hostilities. Figure 3 illustrates an example where military performance increases following a shock, but falls short of desired levels, indicating a resilience deficiency.

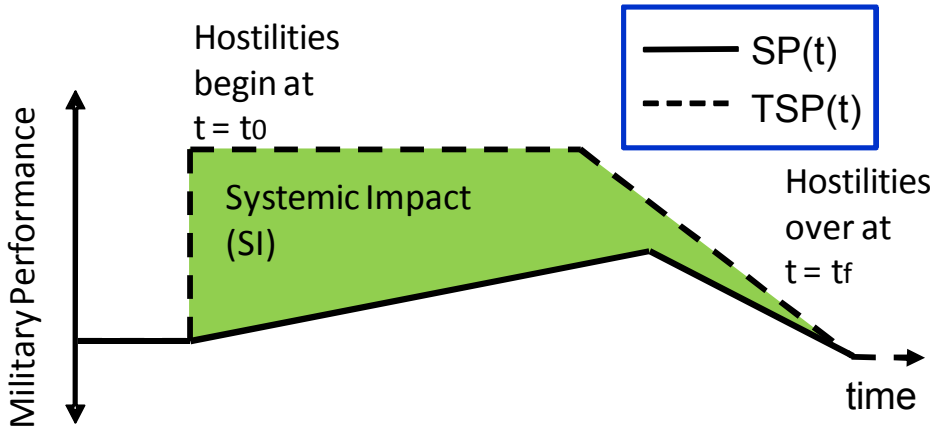

Figure 3: Illustration of systemic impact when targeted system performance increases

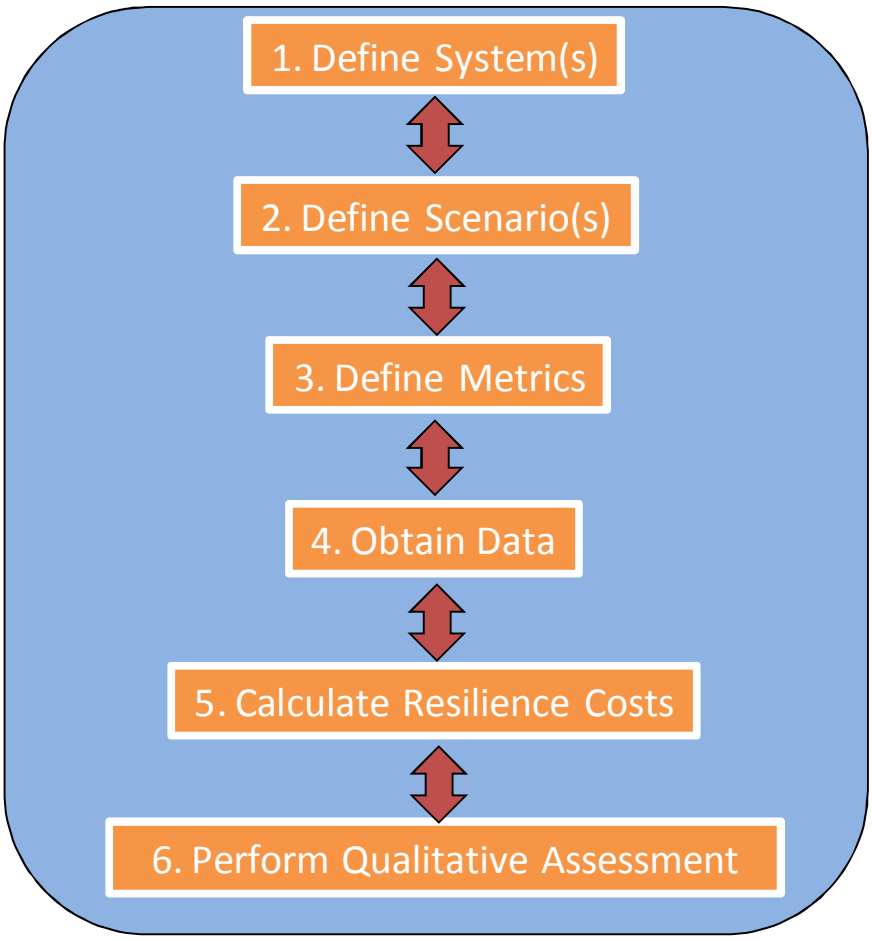

Figure 4: Illustration of the Resilience Assessment Process

After a number of case studies had been conducted using the resilience framework, a resilience assessment process was identified (Warren and Vugrin, 2010). Figure 4 illustrates this process. The resilience assessment process uses six steps to assess resilience of a specific system to a specific scenario. The steps are not necessarily linear—information learned in a later step can be used to iterate back to a previous step. It is important that a variety of subject matter experts be involved in the process because they can add new perspectives that trigger a reexamination of previous assessment steps. The assessment process focuses on obtaining data about system performance. In previous applications, this data has most commonly been obtained through simulation, but historical data has also been used. Mental models could also be used to generate qualitative descriptions that could be used in place of actual data when data is too difficult or uncertain to obtain otherwise.

The last step of framework (6. Perform Qualitative Assessment) refers to the qualitative methodology described in Vugrin, et al. (2010). The authors identified three "resilience capacities" that are produced via features of systems called "resilience enhancement features". This step enables analysts to identify resilience-enhancing improvements to systems, thereby linking the resilience assessment process to foresight. Figure 5 below identifies these three capacities, and the definitions follow:

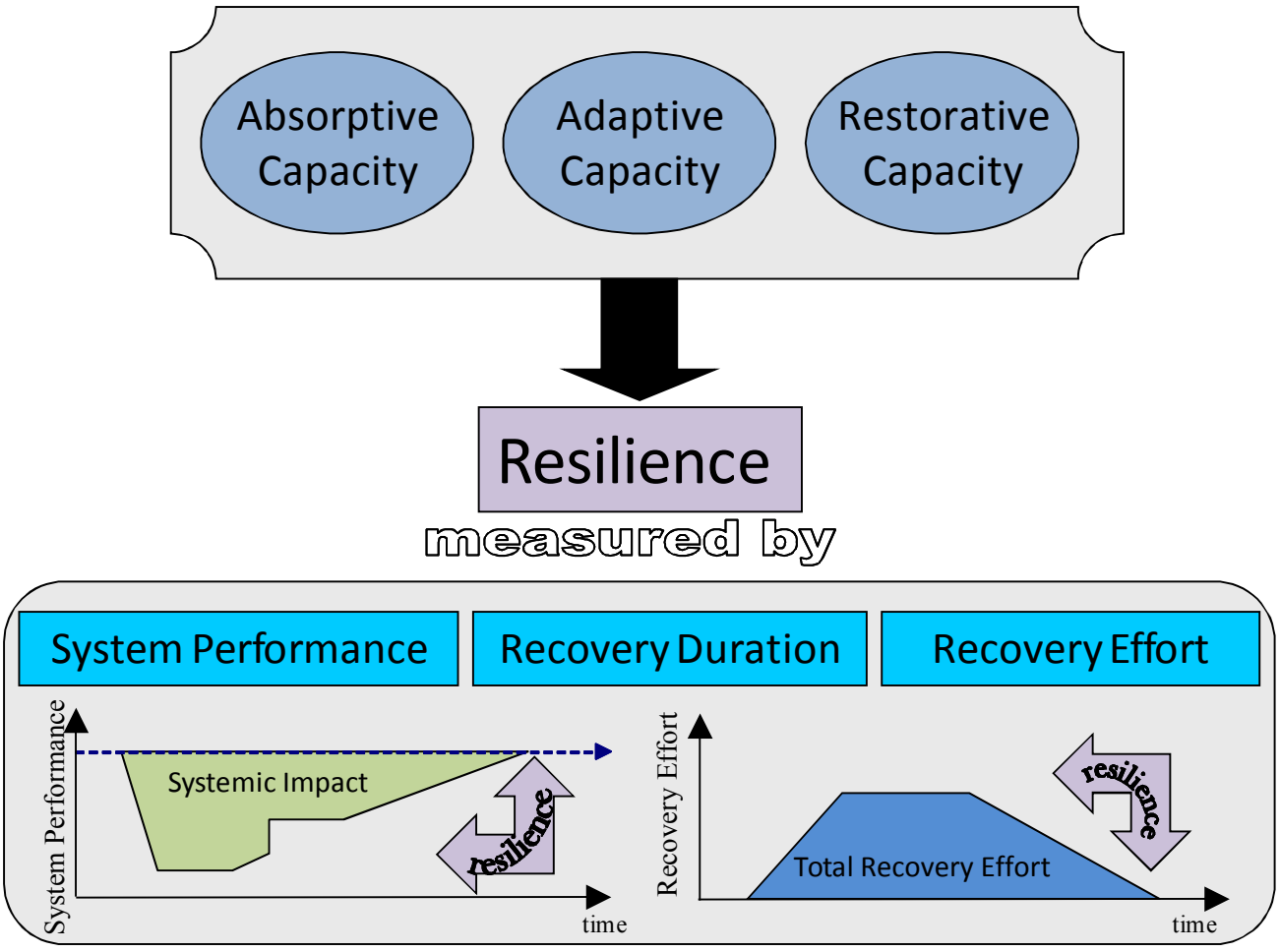

Figure 5: Resilience Capacities Determine Resilience to Shocks

Absorptive Capacity is the degree to which a system can automatically absorb the impacts of system perturbations and minimize consequences with little effort (Vugrin, et al., 2010, p. 99).

Suppose a national security scenario involves the emergence of a new international threat (the shock). A nation will be able to absorb that shock better if it has capable diplomats in place in both adversary and allied countries, military capacities in place to deter the threat, and intelligence capabilities in place to learn more about the threat.

Adaptive Capacity is the degree to which the system is capable of self-organization for recovery of system performance levels. It is a set of properties that reflect actions that result from ingenuity or extra effort over time, often in response to a crisis situation. It reflects a dynamic ability of the system to change endogenously throughout the recovery period (Vugrin, et al., 2010, p. 100). Successful foresight should arm policymakers with capabilities of forging creative, on-the-fly diplomatic and military solutions to minimize systemic impact and the costs of reacting to the threat. Diplomatic solutions can help forge win-win solutions that allow a crisis to deescalate, while military solutions (e.g., mobilizing forces) may be used to deter an adversary or influence its benefit-cost calculations.

Restorative capacity is the ability of a system to be repaired easily (Vugrin, et al., 2010, p. 101). When shocks are disasters, this is simply the ability to repair the structure of the system and perhaps improve it at the same time. National security shocks are often much more complicated. For example, long-term conflicts can be punctuated by many mini-crises where adaptations bring temporary solutions, but the conflict festers. Here, restorative capacity will usually be the ability to resolve the conflict. For example, military power provided the Allies with the restorative capacity to restore peace during World War II. Diplomatic, economic, or political solutions may also resolve conflicts. U.S.-U.K. relations, for instance, remained conflicted throughout the first half of U.S. existence until a number of factors eliminated conflict.

4.2 Correspondence of Resilience to Economics

The equation in Figure 2 shows how resilience costs can be measured for a given set of data that assumes a specific recovery path. More generally, resilience costs will depend upon the specific recovery efforts taken because those recovery efforts affect system performance and determine recovery costs. The following equation describes the optimal resilience problem, where resilience costs are minimized by choosing an appropriate resilience path (adapted from Vugrin, et al., 2010, p. 97):

$$OR = \min_{RE} \frac{\int_{t0}^{tf} [TSP(t) - SP(t)]dt + \alpha \times \int_{t0}^{tf} [RE(t)]dt}{\int_{t0}^{tf} |TSP(t)|dt}$$

This problem is very similar to the problem of dynamic profit maximization by a firm over a discrete period. *TSP(t)* is an exogenous function chosen for the convenience of resilience measurement. A reorganization of this equation (placing exogenous terms into constants c1 and c2) yields:

$$OR = -c_1 + {}^{1}/_{c_2} \times \max_{RE} \left\{ \int_{t0}^{tf} [SP(t)]dt - \alpha \times \int_{t0}^{tf} [RE(t)]dt \right\}$$

This restatement is equivalent to profit maximization between time t_0 and t_f if system performance (*SP*) is revenue and recovery effort (*RE*) is cost. This statement is quite a bit more general since the choice of *RE* is a choice of recovery efforts, which is essentially a nonparametric formulation of actions. In the profit maximization problem, *RE* would be parameterized, for example, to be a firm's

production level, so *RE(t)* would be the cost of producing at that level and *SP(t)* would be the revenue from producing at that level.

This resilience cost problem assumes a relatively short timeframe, so there is no time discounting. However, the problem could easily be generalized to include a discount function to discount both the system performance and recovery effort term.

4.3 Extension of the Resilience Framework to National Security Foresight

The framework presented in Section 4.1 provides a good basis for foresight that rigorously attempts to find ways of improving resilience of systems to particular shocks. The main limitation of the framework is that it looks only at specific events. This would be sufficient if we knew which events were going to occur, but the nature of uncertainty—especially with national security problems—is that the occurrence of future events cannot be known. This section discusses some extensions of the resilience framework to aid in foresight across futures. These extensions will be presented through equations, but will be kept at the conceptual level. Future efforts are needed to increase the mathematical rigor of these extensions.

Because of huge degrees of uncertainty about the future and about how systems operate, and because of the risk aversion of national security organizations, optimality is unlikely to ever be realized but can thought more as a target. The resilience framework discussed in Section 4.1 differentiates "optimal resilience" (OR) and "recovery dependent resilience" (RDR). The latter resilience cost is the result of a particular recovery strategy, thus RDR equals OR only for the optimal resilience strategy.

Let *RDR(s,F)* be a system's expected resilience[3] to scenario s if it has a set of resilience enhancement features *F*. Then, the system's overall expected level of resilience across all scenarios is:

$$TRC(F) = \int [RDR(s,F) \times f(s)]ds$$

TRC is the "total recovery cost," where f(s) is the probability density function for all scenarios *s*. *RDR(s,F)* is the expected resilience for a system with a set of features, *F*, and is measured according to the equation shown in Figure 2.

A profit-maximizing firm will make resilience investments that provide an optimal tradeoff between *TRC(F)* and the costs of investing in features *F*. Maximizing profit (π_{TRC}) is then the choice of an investment in features to solve the following problem:

$$\pi_{TRC} = \min_F \int [RDR(s,F) + C(s,F)] \times f(s)ds$$

where

[3] In this paper, I consider expected resilience only. An obvious extension considers the uncertainty of *RDR* for each scenario. I also do not explicitly consider the timing of different scenarios (and the associated discounting), instead allowing each scenario, *F*, to generally represent a specific set of events at a specific point in time.

$$C(s,F) = \frac{\alpha_2 \times cost(s,F)}{\int_{t0(s)}^{tf(s)} |TSP(t,s)|dt}$$

Here *C(s,F)* are costs for a set of investments, F. The function, $cost(s,F)$, can be considered to be a general cost that is often measured in dollars. The other terms in the equation convert that cost into a resilience cost measured in the same units as *RDR*. The α_2 converts the costs units into the units measured by the RDR equation, similar to the function of the original α. Since both *C(s,F)* and $RDR(s,F)$ have the same denominator and *TSP* is exogenous, optimization requires minimizing the numerators. This formulation allows life-cycle costs to vary over scenarios—if they are constant (i.e., $C(s,F) = C(F)$), then the whole *C(s,F)* term can be moved outside the integral.

Additional constraints can be put on the firm's resilience problem. For example, as discussed in Section 4.6, there is a limit to the losses that a firm will privately consider because it would exceed the value of the firm. A profit-maximizing firm would really consider a piecewise function for every scenario instead of a continuous function that reflects all externalities when the externalities exceed the firm's value.

The firm's problem is conceptually easy, but in reality next to impossible since identifying all scenarios $\boldsymbol{S}$, where $s \in \boldsymbol{S}$ is an impossible task (**S,** after all, is full of "black swans" and "unknown unknowns"), let alone understanding the probability distribution of these scenarios. The model above emphasizes the need to consider probabilities, consequences, and costs jointly. Total resilience is a function of the interaction between probabilities and impacts.

A firm could attempt to address the resilience foresight problem by stovepiping. For example, the firm could rank-order scenarios by probabilities or by impact, only, and make investments that address only the most likely or only the most impactful scenarios. Such strategies would foolishly ignore the interaction between the two factors; the most important scenarios to address are those that are both likely and impactful.

The firm could also stovepipe scenarios and investments. One team could consider investments to increase resilience to hurricanes, while another considers investments to increase resilience to upstream supply-chain disruptions. But such a strategy could result in poor investments since some investments may increase resilience to multiple scenarios, but not appear to be optimal from a stovepiped perspective.

Firms could also stovepipe by allowing each operational organization to consider its resilience separately. This type of stovepiping would likely fail to account for dependencies between operations and result in poor investments.

Because a firm will be unable to completely identify **S** and its probability distribution, the firm's risk management will probably use heuristics to satisfice (i.e., they will make decisions that are "good enough" and do not justify additional effort). To understand the this scenario space, the firm can engage in traditional foresight activities like scenarios, modeling, and gaming to understand both the probabilities and the consequences of different scenarios. Ideally, their examination of scenarios would try to engage in a variety of scenarios to cover the range of scenarios, so that scenarios that have not been considered will be reasonably similar to the scenarios examined. To be sure, it will be impossible to ever assure that this will be true, but engaging with diverse methods and creative people is one strategy that may be promising.

The following matrix groups scenarios based on relative probabilities (high and low) and relative consequences (high and low) to describe where a firm is likely to focus its efforts:

Table 1: A Classification of a Foresight Scenarios

		Consequences	
		High	**Low**
Likelihood	**High**	These scenarios will usually be recognized by a firm because they have a large impact and their frequent occurrence enables an understanding of their likelihood. The firm would likely tackle these foresight problems on an operational level, but the high consequences also are relevant to the strategic level.	These scenarios are also recognized, but not placed at the same level of importance because of the lower consequences. Thus, they will usually be tackled at the operational level.
	Low	These scenarios may result in existential threats to the firm; if the probability is thought low enough, a risk-neutral firm may have incentives to ignore these scenarios or underprovide foresight.	Because these scenarios are relatively unimportant to the firm's bottom line, there will likely be little attention paid by a well-functioning firm.

The matrix for national security organizations can be expected to look similar. Two major differences between the firm and national security organizations involve low-likelihood, high-consequence scenarios.

First, national security organizations, as guardians of public welfare, have an obligation to consider society's risk aversion to high consequence, low probability events and externalities that society incurs from these scenarios. This is not a trivial consideration since it implies that national security organizations must apply a social welfare function or some heuristics that approximate such a function.

Second, national security organizations often consider scenarios driven by adversaries. Unlike natural phenomena (hurricanes, earthquakes, etc.) or scenarios driven by competitive markets, adversaries will choose actions dependent upon their expectations of consequence. Thus, the scenario probability distribution term, $f(s)$, in the equation above is not exogenous, like it may be for something like a hurricane. Instead, this term may be endogenous and be a function of resilience. For example,

$$f(s) = f(s, F) = g(RDR(s, F))$$

is a probability function that represents an adversary's strategy to instigate different scenarios. This function may maximize the adversary's utility, which considers the impacts of those scenarios, or be the result of some game-theoretic interaction (e.g., it may represent a mixed strategy). The function *g()* will probably be very complex and represent the solution to the adversary's expected social utility maximization problem (because the adversary is attempting to maximize some measure of utility through its actions). Thus, an intelligent adversary may want to instigate high-consequence scenarios, especially to scenarios to which it believes national security organization is unprepared.

Therefore, a national security organization will need evaluate whether low-likelihood, high-consequence events are truly low-likelihood. To answer this question, national security organizations need to be informed of both the capabilities and the beliefs of the adversary, in addition to understanding the consequences of the events. The complexity of this problem underscores the importance of making investments that improve resilience to a wide range of events.

The endogeneity of an adversary's behavior underscores a major difficulty in foresight—the future is not set in stone, but is a product of past and current actions. This is especially true for national security organizations in the control space and large organizations (like firms) in the voluntary space that have a large degree of power to shape their future. An organization with foresight will create that resilience by improving consequences and taking actions that shift likelihoods to beneficial outcomes. Resilience foresight will be most effective when consequences and likelihoods are both understood to be endogenous.

4.4 Benefit-Cost Analysis to Guide Resilience Foresight

This extension of the resilience framework in Section 4.3 considers both benefits (lower resilience costs) and costs (investment costs). Therefore, benefit-cost analysis (BCA) may serve as a way of conducting resilience foresight when combined with scenario analysis. BCA is often used by policymakers to evaluate whether a policy or investment is cost beneficial by comparing the expected benefits of a decision to the expected costs. This comparison is relatively straightforward when the expected benefits and costs and uncertainty about those expectations can be quantified with a reasonable amount of confidence. For example, likely scenarios in Table 1 will happen frequently enough (or be closely related to frequent scenarios) that reasonable knowledge about expectations and uncertainties is obtainable from past experience and existing knowledge.

For likely scenarios, BCA is usually straightforward, although there are often issues with accuracy (or possibly bias, see Flyvbjerg, Holm, and Buhl, 2002) and issues like discount rates (e.g., the Stern Review's low discount rates for climate change [Stern, 2008] have proven controversial, see Backus, et al., 2010). A more fundamental problem may be accounting for benefits and costs that may exist across a range of domains. A relatively simple example in national security is the B-52, which was originally procured early in the Cold War for nuclear missions. B-52s have certainly contributed to nuclear deterrence (itself difficult to quantify) but have also contributed to many conventional missions. Thus, investment decisions made by stovepiped nuclear mission planners or conventional mission planners alone would create a danger of misinvestment. After all, procuring both a cost-effective nuclear bomber and a cost-effective conventional bomber would likely be much less cost-effective overall. This highlights that even relatively straightforward foresight needs to incorporate a whole-system approach.

BCA is harder to apply to unlikely scenarios because of a lack of information that can be used to quantify consequences uncertainties. Unlikely, low-consequence scenarios are not as much a concern; unfortunately, it is often difficult to predict whether an unlikely scenario will be high or low consequence. The lack of knowledge about unlikely scenarios may lead them to be treated in three ways.

First, unlikely scenarios may be ignored. Ignoring some types of unlikely, high-consequence scenarios may be a prudent decision by a profit-maximizing firm, but it is unlikely to be justified by organizations that act on behalf of a risk-averse public.

Second, unlikely scenarios may be incorporated into BCA using best guesses about costs and benefits. This approach is advocated by Miller and Stewart (2011) who argue that homeland security in the United States has largely ignored the prudent weighing of benefits and costs and led to a massive overreaction over the past ten years.

Third, unlikely scenarios may be considered with "worst case thinking," which Mueller and Stewart (2011) argues leads to overreaction and suboptimal policymaking. Under the worst case, policymakers will tend to overestimate the benefits of investments to combat unlikely scenarios, leading to overinvestment in unlikely scenarios and underinvestment in likely scenarios. On the other hand, using worst-case thinking policymakers will account for the public's risk aversion.

Mueller and Stewart (2011) argue that worst-case thinking is often a result a "political imperative for public officials to 'do something' (which usually means overreact) when a dramatic terrorist event takes place—'You can't just not do anything'" (p. 22). Thus, worst-case thinking is a way that organizations in the control space can build legitimacy with the public (see Figure 1). Mueller and Stewart advocate that policymakers avoid stoking fears and cite examples of U.S. presidents who have avoided overreaction.

Fear is clearly real and has costs both nonpecuniary costs to people's utility (the psychic impact) and costs that can be measured, like the increased deaths from people flying instead of driving to avoid air terrorism (Blalock, Kadiyali, and Simon, 2009). Ignoring the public's fear risks a kind of "technocracy" that is "incapable of understanding the complex historical and cultural factors which were necessary for the creation of modern society," (Schlesinger and Phillips, p. 461). An organization that ignores the public's fear may lose legitimacy.

Recent research into societal resilience suggests a third way, where national security organizations acknowledge the public's fear, but rather than stoking that fear or ignoring it, attempt to minimize the fear by building societal resilience. For example, Elran (2010) examines the resilience of Israeli society to conflicts with Lebanon and Hama, and the Community & Regional Resilience Institute (CARRI)[4] performs research into societal factors that increase resilience to disasters. Such a strategy encourages a more rational consideration of fear.

Similarly, a middle ground between BCA and worst-case thinking should be used to conduct foresight in national security organizations to increase resilience. This fourth choice, BCA informed by worst-case thinking, is based on weighing benefits and costs of various actions, but also an acknowledgement that unlikely events can happen (both negative risks and positive opportunities) and a resilient system needs the capacity to absorb, adapt, and recover from those events. Adams (1993, pp. 137-148) explains that "The major difference between a thing that might go wrong and a thing that cannot possibly go wrong is that when a thing that cannot possibly go wrong goes wrong it usually turns out to be impossible to get at or repair." BCA informed by worst-case thinking helps build resilience by having policymakers acknowledge the things that "might go wrong" and to reconsider decisions that depend on assumptions that things "cannot possibly go wrong." Even if the likelihood of things going wrong is so small that no major investments are justified, the acknowledgement of a possible future may be enough to tweak some other investment so that the cost of something going wrong is merely high, rather than catastrophic.

Whereas the Sandia resilience framework's (Vugrin, et al., 2010) quantitative methodology (Figure 2) focuses on resilience as system performance, the framework's qualitative methodology (Figure 5)

[4] http://www.resilientus.org/

focuses on resilience as the result of structural properties. The key to integrating BCA and worst-case thinking is to identify resilience-enhancing investments that are cost effective and improve the system's absorptive, adaptive, and restorative capacities in a way that reduces the consequences of worst case scenarios. Such investments can be implemented with foresight because they can satisfy a basic business case (through BCA) and improve the resilience of the system, in general. Prudent investments, therefore, require views of the whole system and thinking about futures at all levels of likelihood and consequence.

BCA informed by worst case thinking adds consideration for the risk aversion of society, which is necessary for national security foresight. Furthermore, while BCA may be sensitive to the choices of probabilities (which are inherently difficult to identify for low-probability events) a focus on the resilience of systems via investments to improve its structural capacities means that system performance will be more robust to errors in probability estimates. Such foresight is likely to be robust because it results in a high level of performance across a range of uncertain factors, when optimizations may unstable to that uncertainty.

4.5 Optimal Control Theory to Guide Resilience Foresight

During development of the Sandia resilience framework, the use of optimal control theory was explored (Vugrin, et al., 2010). Further application of optimal control methods has been explored for chemical supply chains in Vugrin, Camphouse, and Sunderland (2009) and for railroad networks in Vugrin, Turnquist, and Brown (2010). A complete discussion of these applications is beyond the scope of this paper, but additional research that finds qualitative insights from this line of research may be useful for guiding foresight.

4.6 Regulation to Increase Resilience in Firms and Improve National Security

This discussion of resilient foresight is also applicable to firms, especially since the private sector is recognized as being critical to national security resilience (Obama, 2010, p. 19). As argued previously, risk aversion in national security organizations can be justified if it reflects risk aversion in society to risks that can only be managed by a national security organization rather than voluntary action by citizens or firms (that is, where risk management is a public good.) Risk aversion in publicly owned firms is usually not justified since the shareholders of firms can manage risks to their own choosing, so the returns of firm should be of primary importance from a socially optimal perspective. That is, firms should be optimizing their long-term returns. A risk-neutral firm may lead justifiably ignore some low-probability events, even if those low probability events could bankrupt the company. Thus, it may be socially optimal for a particular firm *not* to be resilient to sufficiently low probability events.

For a lack of resilience in a firm to be socially optimal, similar conditions to perfect competition would need to hold. Most important is an absence of externalities. It is conceivable that a low probability event that would spell bankruptcy for a firm could also cause externalities to society. The typical solutions to the externality problem (e.g., lawsuits or fines) require that a viable firm exist after the event. But if an event leads a firm into bankruptcy, those lawsuits and fines will have no effect on the preparation of a rational firm since it will already be bankrupt. Furthermore, these

solutions may not be credible for events caused by malicious actors since the primary cause of the externality is not the firm's lack of preparation, but instead the malicious act.

Because the United States decentralizes power across actors in many spaces (see Figure 1), a single entity, like a national security organization, alone cannot assure that societal welfare will be resilient to future risks. Thus, regulation may be necessary to improve societal resilience when certain conditions are met, like the aforementioned externality problem. Some regulatory solutions that might solve this externality problem are:

- **Require firms to take certain precautionary measures to high-consequence, low-probability events or suffer penalties.** This appears to be the solution taken by the Chemical Facility Anti-Terrorism Standards (CFATS). *Interim Final Rule on Chemical Facility Anti-Terrorism Standards* [6 *Code of Federal Regulations* (CFR) Part 27] established "risk-based performance standards for security of chemical facilities" (DHS 2007a). Chemical facilities must prepare vulnerability assessments and Site Security Plans to address those vulnerabilities or be subject to "civil penalties and orders to cease operations" (DHS 2007b). Such a strategy could require that firms conduct resilience assessments and correct deficiencies with resilience improvements. A danger with this strategy is that it places a heavy burden on national security organizations (in this case, DHS) to monitor that appropriate measures are enacted. Firms have an incentive to shirk, especially if the shirking is not discovered until after the event, when the company is bankrupt.
- **Require firms to purchase liability insurance for low probability events.** Purchasing insurance usually implies some degree of risk averseness, so it normally is not socially optimal for publicly-owned firms to purchase insurance. However, if a firm purchases insurance to a low-probability, high-consequence event from a large enough insurer/reinsurer it increases the likelihood that somebody will be around to provide compensation after an event.[5] The insurer will charge the company based upon the company's risk, so the insurer and the insured have an incentive to make socially beneficial preparations. The company will continue to have an incentive to shirk, but the consequences of shirking will be transferred to the insurance company rather than society.
- **Appeal to the legitimacy of the firms.** Firms can build legitimacy by prudently mitigating the externalities they impose during low-probability, high-consequence events. Firms could demonstrate to the public that they are taking appropriate mitigating actions, and could perhaps create neutral bodies that could certify these actions. Thus this solution exists in voluntary space. Firms would continue to have an incentive to shirk in such an arrangement, and there is a danger that a certification body would not truly be neutral but would instead fall victim to a type of regulatory capture.

Another case where it may not be socially optimal for firms to ignore low-probability events is if there are few firms or one type of event may disable a large percentage of all firms. In this case, perfect competition's assumption of a large number of firms is violated, so the loss of a firm or many firms together would have a relatively large impact on the economy. Justification for regulation in

[5] Mayers and Smith (1982) identifies several reasons that a firm would purchase insurance. One reason is that firms may wish to insure against events that will cause them to go bankrupt and impose large bankruptcy transactions costs.

these cases is weaker than in the externality case because harm would tend to be economic only and could be better managed by other firms and consumers who purchase the firm's or firms' output (the departure of firms from a market can be expected to lead to a new, efficient market equilibrium after demand and prices adjust to the new supply). However, there may be some types of production where normal prices do not properly reflect overall importance (i.e, total consumer surplus). For example, food is relatively cheap, but if a large proportion of food supply were disrupted, many people could die. Presumably the prices would adjust to reflect this importance after-the-fact, but the prices would probably be nonlinear because at some point demand for food is price inelastic (people are probably willing to pay large sums for a minimal amount of food). Thus, the current modest prices of food do not reflect the change in value that would result from a much more than marginal change in supply. Such a situation would surely create a profit opportunity for firms, but firms are unlikely to enter the market as a backstop supplier for two reasons. First, by definition the event is of such a low probability that risk neutral firms have ignored it. Second, following catastrophic events, government regulations or pressure often restrict prices increases, thus there is little incentive for a profit-maximizing firm to be a backstop supplier.

Good governance requires that regulators be fairly conservative about regulating by choosing to regulate to events that are sufficiently low-probability and place a sufficiently high-consequence on society that cannot be mitigated without government intervention (i.e., cases where risk and resilience management are public goods). Even risk-neutral firms have risk management functions that help the company prepare for many (or even most) catastrophic events. Provided that firms have complete information, economic theory would predict their preparatory actions to be socially optimal. If firms do not have complete information, there may be a role for national security organizations to provide additional information as a public good. Some of the relevant information that firms may be missing may be secret, in which case the government needs to weigh the benefits against the costs of releasing the information. When secret information would be too costly to publicly release (e.g., information about specific threats) there may be increased justification for regulators to require firms take specific actions that would be prudent for the firm to take if they knew the secret information.

Prudent risk management by firms should reduce the cases where government intervention is justified. It will be most economical for firms to implement resilience enhancing features that increase resilience to many different types of higher-consequence, medium- and high-probability events. If features are chosen by conducting BCA informed by worst-case thinking, these features are likely to have an additional benefit of increasing resilience to many types of low-probability events as well. A firm with prudent foresight may thereby enhance its resilience to all possible events.

5 CONCLUSIONS

This paper has explored the economics of foresight in national security organizations. Traditional economic firms and national security organizations are similar in many ways; so much of this research is applicable to both types of organizations. The key difference between the two types of organizations is that firms are typically not risk averse, while the decisions of national security organizations should reflect social welfare and society's risk aversion to some events that cannot be mitigated through markets. Unfortunately, foresight to increase resilience is more challenging in national security organizations than in firms.

This paper concludes that national security organizations should have a goal of increasing the resilience of society to both future risks and future opportunities. Resilience may be increased through a process of benefit-cost analysis that considers worst-case scenarios. The resulting policy decisions are prudent (cost effective, though not necessarily optimal) and robust to a range of futures.

There are two primary lines for future research. First, the mathematical extensions of an existing resilience framework have only been extended at a basic level. Additional efforts to fill in the mathematical details will allow quantitative case studies, the development of quantitative tools, and would likely result in new insights about resilience and foresight. Second, processes to conduct foresight across national security organizations need to be improved. This paper has identified some processes that have already been developed, but improving the foresight capabilities of national security organizations is likely to require a combination of government reforms and new techniques and strategies to conduct foresight. The challenge of this problem cannot be understated; there are many inherent features that make government foresight difficult. Improvements may be difficult to identify and implemented owing to the complex relationships in the triad of resources in which national security organizations operate.

6 REFERENCES

Adams, Douglas, 1993, *Mostly Harmless*, New York, Harmony Books.

Amihud, Yakov and Baruch Lev, 1981, "Risk Reduction as a Managerial Motive for Conglomerate Mergers," *Bell Journal of Economics*, v. 12(2), pp. 605-617.

Aspen Institute Business and Society Program, *Overcoming Short-Termism: A Call for a More Responsible Approach to Investment and Business Management,* New York: Aspen Institute Business and Society Program, September 9, 2009.

Backus, George, Thomas Lowry, Drake Warren, Mark Ehlen, Geoffrey Klise, Verne Loose, Len Malczynski, Rhonda Reinert, Kevin Stamber, Vince Tidwell, Vanessa Vargas, and Aldo Zagonel, 2010, *Assessing the Near-Term Risk of Climate Uncertainty: Interdependencies among the U.S. States*, SAND2010-2052, Albuquerque: Sandia National Laboratories, April, 2010.

Bergen, Peter and Laurie Garrett, 2006, *Report of the Working Group on State Security and Transnational Threats,* Princeton, N.J.: The Princeton Project on National Security.

Blalock, Garrick, Vrinda Kadiyali, and Daniel H. Simon, 2009, "Driving Fatalities After 9/11: A Hidden Cost of Terrorism," *Applied Economics,* v. 41(14), pp. 1717-1729.

Coddington, Alan, 1982, "Deficient Foresight: A Troublesome Theme in Keynesian Economics," *American Economic Review,* v. 72(3), pp. 480-487.

Committee on Risk-Based Approaches for Securing the DOE Nuclear Weapons Complex, 2011 *Understanding and Managing Risk in Security Systems for the DOE Nuclear Weapons Complex (Abbreviated Version)*, National Research Council of the National Academies Washington, D.C.: The National Academies Press.

DHS (U.S. Department of Homeland Security), 2007a, "Chemical Facility Anti-Terrorism Standards; Final Rule, 6 CFR Part 27," *Federal Register*, 72 (67), April 9, 2007, pp. 17687-17745.

DHS (U.S. Department of Homeland Security), 2007b, "Appendix to Chemical Facility Anti-Terrorism Standards, 6 CFR Part 27," *Federal Register*, 72 (223), November 20, 2007, pp. 65396-65435.

DHS (U.S. Department of Homeland Security), 2010, *DHS Risk Lexicon: 2010 Edition*, Washington, D.C.: Department of Homeland Security Risk Steering Committee, September 2010.

Elran, Meir, 2010, "Benchmarking Civilian Home Front Resilience: Less than Meets the Eye," in *Strategic Survey for Israel 2010*, eds. Shlomo Brom and Anat Kurz, Tel Aviv: Institute for National Security Studies, http://www.inss.org.il/upload/(FILE)1283331920.pdf.

Eisenhower, Dwight D., 1961, "Farewell Radio and Television Address to the American People," T*he American Presidency Project*, John T. Woolley and Gerhard Peters, eds., accessed May 3, 2011 at http://www.presidency.ucsb.edu/ws/?pid=12086.

Fama, Eugene F., 1980, "Agency Problems and the Theory of the Firm," Journal of Political Economy, v. 88(2), pp. 288-307.

Flyvbjerg, Bent, Mette Skamris Holm, and Soren Buhl, 2002, "Underestimating Costs in Public Works Projects: Error or Lie?" *Journal of the American Planning Association*, v. 68(3), pp.279-295.

Gustavsson, Sten-Olof, 1984, "Flexibility and Productivity in Complex Production Processes," *International Journal of Production Research*, v. 22(5), pp. 801-808.

Hamel, Gary and C.K. Prahalad, 1994, *Competing for the Future,* Boston: Harvard Business Press.

Hartley, Keith, 1997, "Defence Markets," *IEA Economic Affairs*, v. 17(4), pp. 22-27.

Hayek, Friedrich A., 1945, "The Use of Knowledge in Society," *American Economic Review,* v. 35(4), pp. 519-530.

Helmer, Olaf, 1967, *Analysis of the Future: The Delphi Method*, P-3558, Santa Monica, CA: The RAND Corporation.

Ingraham, Patricia Wallace, 2006, "Building Bridges over Troubled Waters: Merit as a Guide," *Public Administration Review*, July/August, 2006, pp. 486-495.

Joint Chiefs of Staff, 2001, *Doctrine for Joint Operations*, Joint Publication 3-0, Arlington, VA: U.S. Department of Defense Joint Chiefs of Staff.

Knight, Frank H., 1921, *Risk, Uncertainty, and Profit*, Boston, MA: Hart, Schaffner & Marx.

Koliba, Christopher J., Russell M. Mills, and Asim Zia, 2011, "Accountability in Governance Networks: An Assessment of Public, Private, and Nonprofit Emergency Management Practices Following Hurricane Katrina," *Public Administration Review,* March/April 2011, pp. 210-220.

Machol, Robert E., 1965, "Methodologies of System Engineering," in System Engineering Handbook, Robert E. Machol, ed., New York: McGraw-Hill, pp. 1-3–1-13.

Mayers, David, and Clifford W. Smith, Jr., 1982, "On the Corporate Demand for Insurance," *Journal of Business,* v. 55(2), pp. 281-296.

Mueller, John and Mark G. Stewart, 2011, "Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security," presented at the Annual Convention of the

Midwest Political Science Association, Chicago, IL, April 1, 2011, accessed at http://polisci.osu.edu/faculty/jmueller/MID11TSM.PDF, last accessed April 6, 2011.

National Committee on Public Service, 2003, *Urgent Business for America: Revitalizing the Federal Government for the 21st Century,* Report of the National Commission on the Public Service, January 2003.

National Intelligence Council, 1998, *Global Trends 2025: A Transformed World*, NIC 2008-003, Washington, D.C., U.S. General Printing Office.

Nordhaus, William D., 1975, "The Political Business Cycle," *Review of Economics and Statistics,* v. 32(130), pp. 169-190.

Obama, Barack, 2010, *National Security Strategy,* Washington, D.C.: White House, May 2010.

Poterba, James M and Lawrence H. Summers, 1995, "A CEO Survey of U.S. Companies' Time Horizons and Discount Rates," *Sloan Management Review,* v. 37(1).

Prenderast, Canice, 2007, "The Motivation and Bias of Bureacrats," *American Economic Review,* v. 97(1), pp. 180-196.

Project on National Security Reform, 2008, *Forging a New Shield: Executive Summary*, Arlington, VA: Project on National Security Reform, November, 2008.

Random House, 2011, "foresight," *Dictionary.com Unabridged*. Random House, Inc. http://dictionary.reference.com/browse/foresight, accessed: April 26, 2011.

Schelling, Thomas C., 2005, "An Astonishing Sixty Years: The Legacy of Hiroshima," Prize Lecture, December 8, 2005, in *The Nobel Prizes 2005*, Karl Grandin, ed., Stockholm: Nobel Foundation, 2006, pp. 365-375.

Schlesinger, James R. and Almarin Phillips, 1959, "The Ebb Tide of Capitalism? Schumpeter's Prophecy Re-examined," *Quarterly Journal of Economics*, v. 73(3), pp. 448-465.

Schmidt, G. and Wilbert E. Wilhelm, 2000, "Strategic, Tactical and Operational Decisions in Multi-National Logistics Networks: a Review and Discussion of Modelling Issues," *International Journal of Production Research*, v. 38(7), pp. 1501-1523.

Schwartz, Norton A. and Timothy R. Kirk, 2009, "Policy and Purpose: The Economy of Deterrence," *Strategic Studies Quarterly,* Spring 2009, pp. 11-30.

Stern, Nicholas, 2008, "The Economics of Climate Change," *American Economic Review*, v. 98(2), pp. 1-37.

Thompson, James R., 2006, "The Federal Civil Service: The Demise of an Institution," *Public Administration Review*, July/August, 2006, pp. 496-503.

U.S. Air Force College of Aerospace Doctrine, Research and Education (CADRE), 1997, *Air and Space Power Mentoring Guide, Vol. 1*, Maxwell AFB, AL: Air University Press.

Vego, Milan N., 2009, *Joint Operational Warfare Theory and Practice*, Washington, D.C.: Government Printing Office.

Vugrin, Eric D., R. Chris Camphouse, and Daniel Sunderland, 2009, *Quantitative Resilience Analysis Through Control Design*, SAND2009-5957, Albuquerque: Sandia National Laboratories, September, 2009.

Vugrin, Eric D., Mark A Turnquist, and Nathanael J. K. Brown, 2010, *Optimal Recovery Sequencing for Critical Infrastructure Resilience Assessment*, SAND2010-6237, Albuquerque: Sandia National Laboratories, September, 2010.

Vugrin, Eric D., Drake E. Warren, and Mark A. Ehlen, 2011, "A Resilience Assessment Framework for Infrastructure Systems: Quantitative and Qualitative Resilience Analysis of Petrochemical Supply Chains to a Hurricane," *Process Safety Progress,* Forthcoming, Published online March 14, 2011.

Vugrin, Eric D., Drake E. Warren, Mark A. Ehlen, and R. Chris Camphouse, 2010, "A Framework for Assessing the Resilience of Infrastructure and Economic Systems," in *Sustainable and Resilient Critical Infrastructure Systems: Simulation, Modeling, and Intelligent Engineering*, K. Gopalakrishnan and S. Peeta, eds., New York, NY: Springer-Verlag.

Warren, Drake E. and Eric D. Vugrin, 2010, *Chemical Supply Chain and Resilience Project: Application of Resilience Assessment Framework to a Historical Case Study,* Albuquerque, NM: Sandia National Laboratories, August 2010.

Zakheim, Dov, 2011, "Confessions of a Vulcan: An Insider's Story of How the Bush Administration Lost Afghanistan," *Foreign Policy*, May 13, 2011.