The Thesis Committee for John Charles Collier
Certifies that this is the approved version of the following Thesis:

Definitions, Frameworks, Modeling Techniques, and Current Practices of System Resiliency

APPROVED BY
SUPERVISING COMMITTEE:

Zhanmin Zhang, Supervisor

Randy Machemehl

Definitions, Frameworks, Modeling Techniques, and Current Practices of System Resiliency

by

John Charles Collier

Thesis

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Science in Engineering

The University of Texas at Austin
May 2019

Dedication

This thesis is dedicated to my family and friends who encouraged and supported me along throughout my time at The University of Texas at Austin.

Acknowledgements

The author acknowledges Dr. Zhang and Dr. Machemehl for their advice and support throughout the thesis writing process. Srijith Balakrishnan and Stephanos Politis also provided sound suggestions and guidance while putting this thesis together.

Abstract

Definitions, Frameworks, Modeling Techniques, and Current Practices of System Resiliency

John Charles Collier, M.S.E.

The University of Texas at Austin, 2019

Supervisor: Zhanmin Zhang

Resiliency research and implementation has become a topic of importance to academia, the US government and industry in the light of the increased number, type and frequency of natural and manmade disasters faced by communities within the United States. The term resilience has so many definitions and methods to model or assess that the idea is almost meaningless without the context of the objectives of the research being conducted or policy being implemented. The lack of unified effort to establish or develop a coordinated resiliency improvement strategy, assessment methodology or a quantifiable prioritization framework for resource allocation makes the implementation of resilience a difficult task, at best, for community decision makers and infrastructure managers. This study identifies current issues with resiliency improvement or enhancement, discusses the application of technology to resilience improvement and provides actionable recommendations to improve resiliency efforts at all levels of government.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

September 11, 2001 significantly impacted the global community by highlighting issues with how the government, local communities, academia and industry viewed the status of the systems and infrastructure relied upon for daily life (O'Rourke, 2007; Ouyang *et al.*, 2012). In the years following September 11, 2001 technology, as well as modifications to infrastructure management and governance, have made our society's infrastructure, social and economic systems more interconnected, complex and relied upon for everyday life (Longstaff *et al.*, 2010; Ouyang *et al.*, 2012). Social, economic and physical infrastructure systems are more capable, but are also more reliant on the other previously disconnected entities (nodes, facilities, organizations, physical infrastructure, etc.) within the community in order to function properly (Weijnen & Bouwmans, 2006). Any disruptions within a community are more likely to cause cascading failures that can be disruptive to not only a particular community or region, but can also have social and economic impacts on a national or global scale as seen in the 2003 Northeast Blackout (Minkel, 2008). On top of being more interconnected, the number of natural and manmade disasters or hazards have increased over the past twenty years, which has led governments, local communities, academia and industry to make resiliency and resiliency planning a major concern (Aldrich, 2012; Aldrich & Meyer, 2015; PPD-21, 2013; Guha-Sapir *et al.*, 2004; Nakagawa & Shaw, 2004; Executive Order 13636, 2013). Resilience can be defined, modeled and planned for differently depending on an entity's resources, objectives, viewpoint and overall end state for resiliency considerations. Varying models and definitions for resilience can sometimes clash and lead to inter-agency or interdisciplinary confusion (Larkin *et al.*, 2015; Meerow *et al.*, 2016; Ouyang *et al.*, 2012). This thesis is an attempt to conduct a literature review of resilience from several perspectives, discuss issues with infrastructure and community resilience, review what technologies have the potential to resolve identified issues and provide actionable recommendations to improve infrastructure resilience for community decision makers.

THE VARYING DEFINITIONS OF RESILIENCE

There are many ways to approach the definition of resilience, and therefore there are multiple ways to model, prioritize for and plan for resilience (Meerow *et al.*, 2016; Ouyang *et al.*, 2012). As defined by the Merriam-Webster's dictionary: resilience is the ability to "recover from or adjust easily to misfortune or change," (The Merriam-Webster Dictionary, 2019). The root of the word, "Resilio," is Latin, and means to adapt and "bounce back" from an unfortunate event (Longstaff *et al.*, 2010; Meerow *et al.*, 2016). The Latin root adds complexity to the dictionary definition. Adapt implicates a systems ability to absorb, change and carry on or recover from an adverse event (Cutter *et al.*, 2008; Goerger *et al.*, 2014; Larkin *et al.*, 2015; Ponomarov & Holcomb, 2009). Using a governance perspective, there is also an aspect of preparation for any hazard or negative event that must also be considered for the definition to be complete (Carlson *et al.*, 2012). Social science argues that a proper definition of resilience should include human capital (education of the population, job skills and employment experience of the population), economic capital (ability to mobilize resources) and social capital (mutual trust within a community, social networks of individuals and groups, and the obligation or willingness to engage in mutually beneficial collective action) (Aldrich, 2012; Aldrich & Meyer, 2015; Nakagawa & Shaw, 2004). Multiple viewpoints of resiliency leaves room for interpretation, and therefore, confusion. Vagueness in the resiliency end state and goals of differing agencies makes operationalizing and defining quantifiable goals for resiliency difficult at best (Meerow *et al.*, 2016). The definitions for resiliency will be discussed in the second chapter. The following details background information on why the government, academia and industry have differing definitions for resilience.

Government

The government defines resilience differently depending on which agency you reference and what that individual agency has for goals and mission. The difference in definitions can be partially attributed to governmental agencies partnering with different entities within academia or different research entities, such as, Argonne National Laboratory, The National Institute of Standards and Technology, or the Naval Post Graduate School to define resilience as pertaining to the hiring agency (Carlson *et al.*, 2012; Gilbert, 2010; Longstaff *et al.*, 2010). While the definitions of resilience vary, most researchers seem to agree that a lack of standardization, a central source of data and tools leaves infrastructure facility owners, infrastructure managers and other decision makers without a clear guide to define and measure the resilience of their structures or systems (Carlson *et al.*, 2012; Gilbert, 2010; Longstaff *et al.*, 2010). Research efforts are often duplicated and similar results are concluded as a result of a lack of resilience knowledge management across government agencies.

The lack of consistency and standardization has caused resiliency to become a National priority. On February 12, 2013, President Obama issued Presidential Policy Directive 21 (PPD-21) and Executive Order 13636 (EO-13636) (Presidential Policy Directive 21, 2013; Executive Order 13636, 2013). PPD-21 directs government agencies to strengthen the security and resilience of infrastructure and identifies sixteen critical infrastructure sectors. In addition, PPD-21 defines resilience as, "The ability to prepare for and adapt to changing conditions and withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." The policy identifies which government agency is responsible for the sixteen critical infrastructure sectors and directs the agencies to make critical infrastructure "secure and able to withstand and rapidly recover from all hazards," (Presidential Policy Directive 21, 2013). EO-13636 highlights the cybersecurity aspect of infrastructure resiliency and the need for a secure knowledge management platform (Executive Order 13636, 2013). These directives guide the establishment of the agencies definitions of resilience based on their individual roles or functions and does not dictate that the definition of resiliency in the directive as the governments only definition. Without a uniform and clear-cut end state with quantifiable goals, local, state and federal agencies have a hard time operationalizing and measuring success of their resilience initiatives (Meerow *et al.*, 2016).

Academia

Academia has provided a plethora of definitions for resilience depending on the discipline of the researcher and the goal of the study (Meerow *et al.*, 2016). The number of definitions is nearly matched by the number of types of models used to describe and illustrate the definitions. Some of these definitions and models describe resilience as an inherent property while others view resiliency as an epistemological idea (Francis & Bekera, 2014). Regardless of how academia views resilience, quantitatively describing the idea is a challenge that adds to the confusion of defining and modeling resilience for infrastructure managers and policy makers. Throughout all of the definitions and models five tensions in theory arise. Resilience theoretical tensions are: (1) equilibrium vs nonequilibrium, (2) positive vs negative vs neutral, (3) mechanism of system change, (4) adaptation vs general adaptability, (5) time scale (Meerow *et al.*, 2016). These theoretical tensions will be discussed in Chapter 2.

A variety of methods are used to model resiliency for several different types of systems and networks. Examples of systems or networks modeled include economic networks, ecological systems, infrastructure systems, communication networks, biological systems and social interaction networks. Describing the network is an important step for choosing which type of model to use when describing resilience. The different types of networks modeled are discussed in Chapter 2, however, this paper focuses on describing heterogeneous bi-directional interdependent infrastructure networks. Each academic area uses different models such as agent-based models, heuristic models, network theory and link and node ranking. These models, discussed in Chapter 3, then are used to develop an algorithm to rank infrastructure by priority, or to describe the effects of different components of a system being degraded or destroyed by an adverse event. The most typical graphical depiction of resiliency is the resilience triangle that graphs level of service versus time in order to create an area that can be used to quantify resilience (Bruneau *et al.*, 2003).

Academia provides four typical methods that infrastructure resiliency enhancement can be achieved. Two of the four methods, robustness enhancement and redundancy enhancement, are actions that can be taken prior to a failure to contain or limit effects of external shocks. The first method, or enhancing robustness, is expending resources to improve the strength of the nodes within a network to withstand external shocks. The second method, redundancy, helps the network to contain the consequences of infrastructure node failures to the affected local region, reduces total downtime of the network or system and minimizes the global impacts (Bruneau *et al.*, 2003). The other two methods: resourcefulness and rapidity, refer to actions taken after a failure has occurred to limit the amount of time that the infrastructure nodes are inoperable. Resourcefulness refers to pre-positioning recovery resources, materials and recovery personnel at critical locations to make restoration as fast as possible. Rapidity refers to the speed at which restoration of a node can be completed (Renschler *et al.*, 2010).

Ecologists, biologists and psychologists all provide different ideas on resilience that vary not only in definition, but also in scale. Some studies focus on the individual level resilience, while others focus on collective resilience. This thesis focuses on a community's collective resilience and how to quantify it. In the social science point of view, community resilience as the collective ability of a neighborhood or a defined area to deal with stressors and efficiently resume with the rhythms of daily life through cooperation following a shock. Some social scientists measure community resilience in terms of social, human and economic capital (Aldrich & Meyer, 2015; Nakagawa & Shaw, 2004). Chapter 2 will discuss these ideas further.

Industry

Industry describes resilience for three different areas. First, Organizational Resilience refers to the resilience of the business's organization that can be measured or achieved in several ways depending on the business's role and goals (Aleksić *et al.*, 2013; McManus *et al.*, 2008). Secondly, Resilience in Systems, can be modeled or described for the industrial production process to ensure that individual industry output goals are met regardless of the conditions (Dinh *et al.*, 2012). Finally, Infrastructure Resilience in Industry, is used to describe the logistical processes and systems used to transport goods.

Industry is also concerned with economic resilience as each industry is highly concerned with the economy in which it operates (Adams *et al.*, 2012; Yodo & Wang, 2016).

While industry's resource availability, goals and objectives are often vastly different than that of the government, they are still concerned with the basic principles of resilience to improve business operations, continuity and product delivery to lower the risks associated with operating in today's volatile environment.

GOALS AND OBJECTIVES

There are several literature reviews available on the topic of resiliency. Most governmental decision makers acknowledge the need for resiliency in the management of infrastructure and governmental systems in the face of the multitude of hazards facing our country today. In spite of this, the idea and goals of resiliency still remain opaque and vague to those who manage infrastructure and make decisions regarding the future of infrastructure in this country (Gilbert, 2010; Meerow *et al.*, 2016). This thesis has three main goals that will attempt to separate the study from other literature reviews on the idea of resiliency. First, this thesis will attempt to identify most of the challenges associated with infrastructure resiliency faced by decision makers and infrastructure managers. Second, once resiliency is defined and the problems faced are framed, this study will begin to describe ways in which current and future technologies could be applied to resolve issues currently faced by infrastructure managers and decision makers. Finally, the thesis will outline some actionable recommendations for planners and decision makers to use for future infrastructure management.

Identify Current Issues with Resiliency

Identifying current issues with the application of resiliency ideas to infrastructure and governmental systems requires a clear understanding of how resiliency is currently defined and the practices in use to improve resilience. Upon this being identified and outlined the issues of current resiliency practices can be identified and recommendations for improving current practices can be established. Some issues are easily solved and the improvements can be actioned easily, while other suggestions would require significant political capital and legal review prior to implementation.

Application of Technology to Solve Current Resiliency Issues

Once the problem is framed and major issues are identified the paper will review what technologies are currently available, or in development, that may be promising for improving infrastructure resilience. The recommendations provided in this thesis on the application of technology to resolve resiliency issues is intended to provide decision makers with ideas for future resiliency improvement investments. The technologies listed are not meant to be "all encompassing," and are simply a means of initiating ideas for improving the application of technology to infrastructure systems. Suggestions may be expensive to incorporate, but they could be incorporated over time to help improve the resilience and efficient management of infrastructure.

Provide Actionable Recommendations for Decision Makers

Finally, the paper will use the review of resiliency literature combined with the identified issues and ideas for the application of technology to resilience issues in order to outline and provide actionable recommendations to decision makers, policy makers and infrastructure managers. The amount of differing definitions, models and resiliency goals often make resiliency a difficult problem to frame (Meerow *et al.*, 2016). Additionally, most academic papers are hard to turn into actionable plans due to their theoretical nature and disconnect from what is actually occurring at the point of execution or in the management of infrastructure systems. This paper will attempt to provide realistic and practical recommendations that can be operationalized by those currently managing the improvements to resilience of infrastructure systems.

SCOPE AND ORGANIZATION

As described above resilience is a vast topic that can be studied in detail for every idea identified. In order to better frame the problem and actually produce actionable recommendations, the scope of resiliency needs to be identified. This paper will, at times, summarize some issues in order to allow room for recommendations that can be actioned by infrastructure managers and decision makers today.

Scope

This study will focus mainly on the overall definition and goals as applied to community and infrastructure resilience in the United States. Current definitions and practices will be limited, in this study, to efforts being conducted in the U.S. Recommendations for this study will focus on infrastructure resilience and the management thereof, but, some of the recommendations can be applied to other types of systems and networks. This study briefly discusses a review of and differentiates between definitions of resilience, issues with resilience management and the current practices in community and infrastructure resilience management. A short list of current and developing technologies are described giving ideas as to how they can be applied to infrastructure resiliency management. Finally, a short list of possible recommendations based on this study’s findings on ways to improve infrastructure resiliency management are outlined and discussed

Organization

The study is outlined in the Introduction Chapter and is followed by a Definitions and Current Practices of Resilience in Chapter 2. Chapter 2 is a brief literature review and overview of the different resilience policies and practices in use today. Chapter 3 describes different models used in an attempt to quantitatively describe resilience for management and improvement purposes. Chapter 4 identifies issues with the definition and practices of resilience in use today. Chapter 5 describes current technologies and technologies that are in development that can possibly be applied to the management of infrastructure resilience. Chapter 6 identifies further research required to better describe ideas proposed in the study. Finally, Chapter 7 provides conclusions and actionable recommendations for decision makers and infrastructure managers with regard to improving resilience of communities and infrastructure.

Chapter 2. Definitions and Current Practices of Resilience

In the years following September 11, 2001 and Hurricane Katrina in 2005, there has been a noticeable shift from simply protecting infrastructure to ensuring that entire communities are resilient (Nakagawa & Shaw, 2004; O'Rourke, 2007). Community resilience can be defined as the collective ability of a neighborhood or area to deal with stressors and efficiently resume the rhythms of daily life through cooperation following shocks (Aldrich & Meyer, 2015). Incorporating an idea, such as resilience, into real world policy is not easily executed when managing the highly complex and interconnected modern infrastructure systems and communities made of both social and physical entities (O'Rourke, 2007). There is an agreement that communities must be prepared to respond to and recover from the full gambit of threats faced, however, there is a lack of consensus over how to define, measure and assess resilience (Carlson *et al.*, 2012). Due to the lack of a cohesive national effort, federal agencies, along with their state and local counterparts, are implementing individual and parallel ways to address resilience. The parallel nature of addressing resilience leads to duplicated and inefficient efforts in incorporating resilience into policies governing communities and managing infrastructure (Larkin *et al.*, 2015).

This chapter provides a brief literature review of how resiliency is defined by U.S. federal government agencies, academia and industry. The varying approaches to resiliency will be used to illustrate the issues faced by policymakers, infrastructure managers and academic researchers while defining and managing resilience.

GOVERNMENT

In the 1980s concerns about aging infrastructure led the National Council on Public Works to begin focusing on the maintenance and condition of public infrastructure (highways, bridges, water supply facilities, wastewater treatment facilities, etc.). Increased international terrorism in the 1990s led to the evolution of critical infrastructure defined in terms of national security. After September 11, 2001, seventeen critical infrastructure sectors and key assets were listed in the National Infrastructure Protection Plan (NIPP). In 2013, Presidential Policy Directive 21 (PPD-21) reduced the number of critical infrastructure sectors to sixteen by removing postal and shipping services from the list of critical infrastructure sectors (O'Rourke, 2007; The Department of Homeland Security, 2013). PPD-21 and EO-13636 in 2013 tasked federal agencies with improving national resilience. PPD-21 and EO-13636 were motivated by events like Hurricane Katrina, which highlighted the need to update inadequate and inflexible risk-based analysis approaches to disaster management (Presidential Policy Directive 21, 2013; Larkin *et al.*, 2015; Executive Order 13636, 2013; The Department of Homeland Security, 2013). Figure 1 outlines the sixteen critical infrastructure sectors identified by PPD-21.

"There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."
- Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience

Figure 1: The sixteen critical infrastructure sectors from PPD-21 (Presidential Policy Directive 21, 2013).

Risk and resilience are sometimes used synonymously, however the concepts have different meanings. Mitigating the effects of disasters based on risk involves specific performance knowledge or the expectation of individual system components to operate or fail. Risk is often determined by the threat, the vulnerability of an individual system to fail and by the consequence of that individual systems failure. Once this risk is quantified, government decision makers can then predict, manage and mitigate threats based on policy options and resource availability. Often, risk-based decision making has significant impacts on how particular industries or disciplines conduct business (Larkin *et al.*, 2015). The investment in physical infrastructure resiliency improvement is subject to the political environment due to the empirical methods in use today (Aldrich, 2012). Resilience, unlike risk, incorporates a component of time that is not considered in risk-based decision making (Larkin *et al.*, 2015).

Resiliency assessment and quantification for improvement, based on 2013 Presidential orders and directives, is relatively young and is complicated by different agencies creating parallel efforts to define how to conduct resiliency improvement. For example, DHS has a $20 million funding opportunity to create a resiliency center of excellence to research infrastructure resilience at a regional scale, while, at the same time, the National Institute of Standards and Technology (NIST) has a similar twenty million dollar resilience center of excellence to research infrastructure resilience at the community scale (Gilbert, 2010; Larkin *et al.*, 2015). Two different federal agencies funding highly related research projects with different goals and objectives may lead to a variance in the definitions and objectives for resilience at the regional and community levels. The variance in definitions and goals may lead to complications in the policy incorporation process and differences in resiliency resource allocation at the community and regional levels.

Parallel, but disjointed research, while underway, is not providing current decision makers with an interim decision-making tool which will lead U.S. federal agencies to develop interim resilience assessment and management policies. In order for practitioners to be able to govern resilience, a unified, repeatable, quantitative methodology for improving and assessing resilience is required. The interim resilience policies of different U.S. federal agencies, which lack clarity in implementation strategies, have negative impacts that prevent the necessary coordination. As a result of the lack of coordination, cascading failures may be intensified between infrastructure sectors, communities and regions. Different resiliency definitions and understandings between federal agencies also lead to duplicated efforts, discrepancies in guiding principles and assessment techniques, and is detrimental to the development of cohesive national resilience plans or policies (Carlson *et al.*, 2012; Gilbert, 2010; Larkin *et al.*, 2015; Longstaff *et al.*, 2010).

U.S. federal agencies have created governable resilience assessment and management frameworks. These frameworks differ based on the mission of the agency and the goals associated with accomplishing that mission (Larkin *et al.*, 2015). Resilience assessment and management frameworks can also differ within the larger federal agencies. The Department of Defense (DOD) and DHS, for example, have broad missions and are large organizations consisting of many different "sub-departments." The "sub-departments" can define and approach resiliency differently depending on their role within the larger federal agency (Goerger *et al.*, 2014; The Department of Homeland Security, 2013).

Simplifying the complicated web of definitions and differing approaches can be done by identifying an agency to take the lead on resiliency based on the federal agency with the most applicable mission statement and role in improving resiliency in the United

States. Once the lead is identified that specific agencies definition of resiliency and methods for quantifying resiliency should be used or adapted for use by other federal agencies. Below identifies a possible federal agency to take the lead on resiliency and how each other federal agency's mission and role fits into each aspect of that federal agencies' definition of community and regional resilience.

Unified Definition of Community and Infrastructure Resilience

The only federal agency that has resiliency explicitly as a part of its mission statement and has the broadest responsibility within the US homeland is the Department of Homeland Security (DHS). The DHS mission is "to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards,"(The Department of Homeland Security, 2019; The Department of Homeland Security, 2013). Since they are expressly tasked with resilience their definition should be considered as a front runner when looking for a unified definition. This thesis will focus on the DHS definition of resiliency and describe how other federal agencies fall into the different approaches to resiliency mentioned in the DHS approach.

The Argonne National Laboratory, who partners with the DHS defines resiliency as: "the ability of an entity-e.g., asset, organization, community, region-to anticipate, resist, absorb, respond to, adapt to and recover from a disturbance," (Carlson *et al.*, 2012; Fisher *et al.*, 2010). Argonne National Laboratory's definition of resilience illustrates that resiliency, unlike risk, includes a consideration for actions taken before, during and after a significant event. The National Academy of Sciences (NAS) is less detailed in their definition by grouping actions taken before an event into an entities' ability to "plan and prepare for" an event (Larkin *et al.*, 2015). The NAS definition is more focused on a systemic approach and does not mention the ability to “resist,” or to thwart attacks and manmade disasters (Carlson *et al.*, 2012). The difference between the Argonne National Laboratory and the NAS definitions is one specific example of how varying definitions, though seemingly small, can have a significant impact on how an entity prepares for and defines resilience.

According to most literature community and regional resilience can be broken down into several subsystems some of which are: economy, civil society, critical infrastructure, supply chains and governance. DHS proposed a Regional Resilience Assessment Program (RRAP) in 2009 that can be used to assess resilience across the spectrum of government responsibilities (The Department of Homeland Security, 2013). Using the Argonne National Laboratory’s definition of resilience described above, resiliency activities can be broken down into four main components or indices. The four indices, which are part of a newly proposed Resilience Measurement Index (RMI) are preparedness, mitigation, response and recovery (Carlson *et al.*, 2012; Fisher *et al.*, 2010). Each federal agency and their “sub-departments” focus on one or more of these aspects and can be associated to each according to their mission.

The economic subsystem is composed of people, firms and institutions that interact to accomplish the production, distribution and consumption of goods and services. The economy is considered resilient based on the ability of the system to recover from severe shock inherently and adaptively. The civil society sub-system is the formal and informal modes of social organization and collective action outside of government authority (examples include unions, health and human service organizations, religious organizations etc.). The civil society sub-system describes the public’s ability to adapt to, respond to and recover from a disturbance. The critical infrastructure subsystem is the network used for providing goods and services. Critical infrastructure resilience is the ability of those subsystems to mitigate and minimize the loss in functionality and delivery of goods and services after a disturbance. The supply chain subsystem is the capability of supply chain operator's to exchange value with partner supply chain operators inside and outside the impact area in both the public and private sectors. Measures of supply chain resilience include redundancy, flexibility, density, complexity, node criticality and public-private partnerships. The supply chain subsystems exist in the physical and cyber realms. The governance subsystems are the public organizations that contribute to the administration of government functions to the community and the process through which government institutions make decisions. Governance resilience is a function of the community's ability to reduce risk, engage local residence on mitigation, create organizational linkages and protect and enhance social systems (Adams *et al.*, 2012; Carlson *et al.*, 2012; Fisher *et al.*, 2010).

Each subsystem has implications for some if not all of the four indices of the RMI and different federal agencies have responsibilities in one or more of the subsystems mentioned. Each approach or part of resiliency will be discussed along with the subsystems that have implications in each. Along with that some of the federal agencies responsible for that subsystem will be identified by index and subsystem (Presidential Policy Directive 21, 2013; The Department of Homeland Security, 2013).

Preparedness

Preparedness is the activities taken by an entity to define and address the hazards present in the entity's environment prior to a hazard event. Preparedness addresses the anticipation of a disturbance (Carlson *et al.*, 2012). The subsystems that are affected by preparedness are the economy and governance. All federal agencies work toward improving preparedness of communities and infrastructure governance. The main federal agencies that have a responsibility to ensure economic resiliency include but are not limited to the DHS, the Department of the Treasury, the Department of Commerce, the Department of Agriculture and the Department of Transportation (Larkin *et al.*, 2015).

Mitigation

Mitigation is the activities taken prior to an event to reduce the consequences and severity of a hazard (Carlson *et al.*, 2012). Mitigation addresses the ability to resist and absorb a disturbance. The subsystems effected in mitigation are the economy, civil society, supply chain and governance. All federal agencies work toward improving mitigation of communities and infrastructure governance. The main federal agencies that have a responsibility to ensure civil society and supply chain resiliency include but are not limited to the DHS, the Environmental Protection Agency (EPA), the Department of Health and Human Services, the Department of Transportation, the Department of the Interior, the Department of Defense/US Army Corps of Engineers and the U.S. Department of Agriculture (The U.S. Army Corps of Engineers, 2016; Larkin *et al.*, 2015).

Response

Response is the immediate and ongoing activities, systems and programs that have been developed to manage the adverse effects of an event. Response addresses the ability to respond and adapt to an event (Carlson *et al.*, 2012). All Subsystems are affected during response. The federal agencies responsible for the critical infrastructure subsystem include but are not limited to the Department of Transportation, the DHS, the EPA, the Department of Interior and the Department of Defense/U.S. Army Corps of Engineers (The U.S. Army Corps of Engineers, 2016; Larkin *et al.*, 2015).

Recovery

Recovery is the activities and programs designed to effectively and efficiently return conditions to a level acceptable to the entity (Carlson *et al.*, 2012). In some cases, the pre-disaster conditions are not acceptable operating conditions and the system or network, must be upgraded to meet new demands. The idea that reaching a single state of equilibrium in order to be considered recovered may only apply to a few systems or networks. In order to be resilient, systems need to be recovered in a way that allows for a dynamic and flexible state that can adapt to new post disruptive conditions (Meerow *et al.*, 2016). Social scientists argue that spending money on physical infrastructure resilience is not enough and that resources and effort need also to be spent on the social capital aspect in order to deem a community resilient. During recovery it is suggested by social scientists that community members be evacuated together, or reunited at the earliest possible time in order to allow a community to utilize social capital to begin to recover even if they are still at an evacuation location and not at home (Aldrich, 2012; Nakagawa & Shaw, 2004). All subsystems are affected during recovery and all federal agencies have a role in the recovery approach planning.

ACADEMIA

Resilience research in academia stems as far back as the 1800s in disciplines like psychology and physiology (Tusaie & Dyer, 2004). The concept of resiliency has evolved and is now applied to more disciplines such as engineering, ecology, social science and economics. As the interest in developing resilience in communities and infrastructure grows and evolves, the number of different definitions grows to the point where the term resilience is almost meaningless without the context of who is conducting the research, why the research is being conducted, when the research was conducted, what the research was conducted on and where it was conducted (Klein *et al.*, 2003; Meerow *et al.*, 2016). According to Meerow (2015), five main conceptual tensions are present throughout literature concerning the definition of resilience: 1) the understanding of system equilibrium, 2) positive vs negative vs neutral conceptualizations of resilience, 3) the mechanism of system change, 4) general adaptability vs adaptation, 5) the timescale of the change.

The idea of resilience being applied to infrastructure and communities was first introduced by Holling (1973), who was approaching resilience from an ecological standpoint. Holling described resilience as the ability of an ecological system to "persist" when changed. The term "persist" implies that the system did not remain the same or return to a steady state equilibrium, which implies that there was more than one equilibrium state (Meerow *et al.*, 2016). The idea of a changed equilibrium state is in contrast to the "engineering" idea of resilience. "Engineering resilience" focuses on a single equilibrium state which a disruption would change and the resilience is measured by determining how long the system took to return to the equilibrium state that existed prior to the disruption. This idea of a single equilibrium does not consider the ability of a system to adapt or change the post event equilibrium state to a better or worse equilibrium state (Meerow *et al.*, 2016). The idea of multiple equilibriums or a constantly changing, or dynamic equilibrium, is often referred to as "ecological" resilience.

A community and its infrastructure are often characterized as being made up of both social and physical systems, or a group of regularly interacting components that makeup a universal whole (Zhang, 2018). In order to understand and quantify the resilience of a system, it is key for a researcher to be able to identify the system under consideration (Francis & Bekera, 2014). While many definitions of what resilience is exist, it commonly implies the ability of a system to return to normal after the occurrence of a disruptive event (Hosseini *et al.*, 2016). As most of the definitions and measures revolve around a disruptive event, it is also important the researcher be able to characterize the disruptive event or set of events that may make the system's normal operations vulnerable to disruption. Most of the time this vulnerability to disruptive events is put in terms of likelihood of occurrence (Francis & Bekera, 2014).

Resilience is often seen as a positive attribute and implies a systems ability to not only maintain functionality, but also to grow and improve. Some argue that resilience is not always a positive concept. If the equilibrium state prior to a disaster is undesirable, then the ability of the system to return to that state is not acceptable. Conditions like dictatorships and poverty levels are examples of systems or networks with equilibrium states that may be undesirable, but resilient. Resilience for "whom," or for "what" are being asked by social scientists using normative judgements to determine what is or what is not a desirable state (Klein *et al.*, 2003; Meerow *et al.*, 2016).

In literature, there are three main mechanisms, or ways cited to achieve resilience. They are: persistence, transition and transformation. Persistence refers to the ability of a system to resist a disturbance to maintain equilibrium. Many definitions of resilience in literature also refer to the ability of a system to adapt or transition to changes in the system's environment or transform to a new environment created by change while maintaining functionality. Adapting refers to incremental changes while transformation refers to a significant change in the equilibrium state (Meerow *et al.*, 2016).

Adaptation is another conceptual tension that relates specific adaptations to known threats with the ability of generic adaptability. Specific adaptations to known threats is "specified" resilience, while general adaptability is "general" resilience. Focusing on specified resilience may limit a system's ability to be flexible and responsive to unexpected threats. Another term used to describe the ability to adapt is "inherent," or the ability to adapt in normal situations vs "adaptive," or the ability to adapt during unexpected detrimental events like disasters. When describing economic systems there is also a distinction between short-term adaptation, or specialization, vs long-term adaptability. In general scholars argue that flexibility and adaptability across the spectrum of both expected and unexpected threats is preferable (Bouch *et al.*, 2012; Carlson *et al.*, 2012; Meerow *et al.*, 2016; O'Rourke, 2007; Stephens *et al.*, 2016).

Some definitions of resilience view the timescale or rapidity of recovery as essential. The focus can either be on rapid onset events or disasters or gradual change such as climatic shifts. The definitions that mention timescale acknowledge the need for rapid recovery post-disturbance or disaster event. The issue with the definitions that emphasize the importance of quickly returning to an equilibrium state do not specify the timescale (minutes vs hours vs days vs months etc.) (Meerow *et al.*, 2016).

Bruneau *et al.* (2003) conceptualized resilience for both social and physical systems as having four qualities: 1) Robustness, 2) Redundancy, 3) Resourcefulness, and 4) Rapidity. (1) Robustness is the inherent strength or resistance in a system to withstand external stressors without degradation or loss of functionality. (2) Redundancy refers to a systems ability to allow for alternate options, sources of services or goods, choices, or substitutions under stress. (3) Resourcefulness is the capacity to mobilize needed resources and services for repair or replacement in emergencies. (4) Rapidity is the speed with which a disruption can be overcome with safety, services and stability restored (Bruneau *et al.*, 2003; O'Rourke, 2007; Renschler *et al.*, 2010).

Economy

There are two types of economic resilience described by Rose (2007), the types are static and dynamic economic resilience. Static economic equilibrium is the capability of a system or node within a system to continue to fulfill its purpose or maintain functionality when faced with a shock. Dynamic economic equilibrium is defined as the speed at which a system recovers from a disturbance to achieve a steady state. Rose's (2007) idea of static vs dynamic economic equilibrium is at odds with most definitions of equilibrium. As discussed previously, other disciplines define static equilibrium as the idea of returning to the state of equilibrium that existed prior to a disturbance while dynamic equilibrium describes a constantly changing definition of steady state or normal operating conditions. Rose and Lao (2005) see economic resilience as an inherent property or ability to adapt that enables firms and regions to minimize the chances of maximum potential losses. Economic resilience is mostly defined as the ability of those involved in the economic sector to adapt to changing conditions after a disturbance to maintain the economy and continue its growth (Hosseini *et al.*, 2016; Rose, 2007).

Social Scientists argue that economic capital is not the only type of capital that is important to community resilience. Human capital and social capital, or the idea of networks that can provide resources based on trust and bonding, are also seen as legitimate forms of capital. For economists, the idea of measuring trust and naming it as "capital" like other "ordinary" capital is unacceptable. Aaron (2000) "capital": 1) extension in time, 2) deliberate sacrifice in the present for future benefit, 3) alienability. He particularly believes that social capital fails to fulfill the second requirement, saying that, “The motives of interaction are not economic,” (Arrow, 2000; Nakagawa & Shaw, 2004).

Engineering

In comparison to other disciplines, the idea of engineering resilience or resilience applied to engineering, is relatively young. The idea can be applied to technical systems ranging from infrastructure networks (electrical grids, road networks, etc.) to tanks and fighter planes. The Society of Mechanical Engineers (ASME) describes resilience as the ability of a system to sustain external and internal disruptions without losing the ability of performing the system’s function, or if disrupted, fully recover functionality rapidly (Hosseini *et al.*, 2016). The DOD describes a resilient system in terms of their mission to equip and deploy military forces needed to deter war and assure national security (DOD website). The missions conducted by the DOD require engineered systems to meet a variety of missions from non-kinetic operations (IE humanitarian assistance or disaster relief) to kinetic operations with near-peer military forces. This range of missions requires a flexibility, adaptability and maintainability that requires and pushes resilient systems beyond their max. The DOD definition for engineered resilient systems is “trusted and effective out of the box, can be used in a wide range of contexts, is easily adapted to many others through reconfiguration and/or replacement and has a graceful and detectable degradation of function,” (Goerger *et al.*, 2014). The idea of graceful degradation is considered more in engineering resilience than in other disciplines because it allows for corrective actions to repair or maintain systems that will inherently degrade over time. Other disciplines, like social sciences, do not necessarily consider degradation of a social system in their definitions of resilience, but rather see it as the disturbance itself.

A number of definitions for engineering resilience have been created. In their research, Allenby and Fink (2005) characterized resilience as “the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must.” Along similar lines, Haimes (2009) defines resilience as “the ability of a system to withstand a major disruption within acceptable degradation parameters and to recover within a suitable time and reasonable costs and risks.” In his research, Hollnagel (2011) leaves the definition a little more generic, “intrinsic ability of a system to adjust its functionality in the presence of a disturbance and unpredicted changes.” Along with the previous definitions of resilience, the American Society of Mechanical Engineers (ASME), developed their own definition of what resilience for a system entails, “ability of a system to sustain external and internal disruptions without discontinuity of performing the system’s functions, or if the function is disconnected, to fully recover the function rapidly” (Allenby, B. & Fink, J., 2005; Carlson et al., 2012; Dinh et al., 2012; Haimes, 2009; Hollnagel, 2011; Hosseini et al., 2016; Meerow et al., 2016; Yodo & Wang, 2016).

The National Infrastructure Advisory Council (NIAC) (Fisher *et al.*, 2010) defines infrastructure system resilience as the ability to anticipate, absorb, adapt and rapidly recover from a disruptive event. Vugrin *et al.* (2011) developed a similar definition to the NIAC definition but limited it to just three key pieces, “function of absorptive capacity, adaptive capacity and restorative capacity.” These two definitions led to the idea and creation of the resilience triangle, which relies on the absorptive capacity, adaptive capacity and restorative capacity of the system, all working together (Francis & Bekera, 2014). Francis *et al.* (2014) goes on to further define each group with the absorptive capacity being the capacity of the system to absorb perturbations and minor consequences without much effort, adaptive capacity being the ability of the system to adjust to undesirable situations by adaptation, and the restorative capacity being how rapid the system can restore itself to its normal operating state (Hosseini *et al.*, 2016; Vugrin & Camphouse, 2011).

Infrastructure resilience can be seen as a subset of both the social sciences as well as the economy because the failure of infrastructure systems can have a negative impact on a community and its economy. Interdependencies within the infrastructure network and in the community highlight the complexity and the bi-directional nature of failure consequences and shows that infrastructure performance can be measured in both the physical engineering terms and in terms of societal impact (Hosseini *et al.*, 2016).

Social Science

Social sciences look at resilience capacities of individuals, groups, communities and environments. The community and regional resilience institute defines resilience as the ability to predict risk, reduce adverse consequences and return rapidly through survival, adaptability and growth in the face of turbulent changes. Pfefferbaum *et al.* (2007) on the other hand, defines community resilience as “the ability of community members to take meaningful, deliberate and collective action to remedy the effect of a problem, including the ability to interpret the environment, intervene and move on.” These two examples of social definitions include both an individual and collective aspect common to social interpretations of resilience. In this thesis psychology, ecology and sociology are subsets of Social Sciences (Gilbert, 2010; Hosseini et al., 2016; Pfefferbaum *et al.*, 2007).

Phycological resilience has some of the oldest definitions of resilience. Resilience in an individual has been studied and described in many ways going back to antiquity with the philosophers practicing stoicism and cynicism to try and describe how to cope with challenges in life (Morris & Morris, 2004). Resilience in this case is an individual's ability to endure hardships and face challenges without losing a sense of purpose or drive for life. Religious leaders and psychologists have been trying to describe resilience for a long time using different terms. Maslow described resilience, or a way to determine resilience, in his hierarchy of needs, but he referred to it as what motivates people (McLeod, 2007).

Biological and ecological resilience are very similar and are studied by health services, biologists and ecologist as well. Resiliency in this case involves the ability of a body or system to respond to, cope with and recover from a threat. Biological and ecological resilience can be related to both economic resilience, as well as, engineered systems definitions of resilience (Hosseini *et al.*, 2016; Perrings & Walker, 1997).

Behavioral and social scientists argue that spending on disaster preparation of physical infrastructure is also not as effective as bolstering social resilience and building on social networks because physical infrastructure improvements are subject to political cycles (Aldrich & Meyer, 2015). Some social scientists refer to social capital as the measure of a community's collective resilience to disruptive events. Hanifan (1916) descried social capital as good will, fellowship, mutual sympathy and social intercourse among a group of individuals and families that make up a social unit. Bourdieu (1985) defined social capital as one of four types of capital (alongside economic, cultural and symbolic) that collectively determine social life trajectories. Bourdieu described social capital as the aggregate of the actual or potential resources that are linked to the possession of a durable network of relationships of mutual acquaintance or recognition used to advance one's position in society or in social conflict. Coleman (1988) focused on how social capital could be turned into actual resources. Lin (1999) tied social capital to networks of relationships showing that resources can be accessed or mobilized through ties in networks. Putnam (1995) defined social capital as the features of social organizations, such as networks, norms and trust that facilitate action and cooperation for mutual benefit. Putnam's definition does not address or consider conflicts within a society (Aldrich, 2011; Aldrich & Meyer, 2015; Nakagawa & Shaw, 2004; Norris *et al.*, 2008; Siisiäinen, 2000).

Aldrich and Meyer (2015) suggest five policy changes that can improve community resilience from a sociological standpoint using the theory of social capital. Social capital can be improved by time banking, community currency, focus group meetings, social events and planning of community layout and architectural structures. Time banking is giving incentives or rewards such as community currency to those who volunteer (1-hour labor for local merchant coupons or currency that can be redeemed at local vendors). Community currency increases general trust within a community by getting locals to interact and can have mental health benefits associated with it as well. Another way to increase social capital is to give the citizens "buy-in" by conducting focus groups and social events. Community "buy-in" increases trust in the system or government. The physical layout of a community can also be designed to facilitate a feeling of belonging amongst the citizenry. Community layouts incorporating areas for the community to mingle, meet, and spend time together increase the social connectivity of a community and leads to an increase in social resiliency (Aldrich & Meyer, 2015). Investing in the social networks and social capital of a community prior to a storm event may significantly improve community resilience.

INDUSTRY

Resilience in industry is defined using different definitions from academia and effected by the regulations and management practices of the government. Industry looks at resilience as a requirement on one hand, and as a way to ensure profit during unexpected events on the other. The government regulates resilience into infrastructure that it deems as critical to national security as well as the national economic security. Some industries are therefore forced to invest in resiliency. Other industrial members that take part in Public Private Partnerships (PPP) for building and managing infrastructure are also mandated to build in resilience. For those industries that are not regulated there is a disincentive to building or designing in resilience because it costs resources and time that cut into profits. The industrial sector is mainly concerned with organizational resilience, industrial process resilience, economic resilience and infrastructure resilience (Clifton & Duffield, 2006; Hosseini *et al.*, 2016; Stewart *et al.*, 2009).

Organizational Resilience

Organizational resilience addresses the need for an industrial entity (firms, businesses, etc.) to respond to rapidly changing business environments. Organizational resilience involves both physical resilience, as well as, resilience in the social realm as well. Businesses with constant turnover need to be able to continue to conduct business, and therefore, must have systems that address knowledge management in order to be able to continue to operate at an expected level. Sheffi (2006) defined organizational resilience as an inherent ability to recover to a steady state allowing an industrial entity to continue normal operations under constant stress or after a disruptive event. Other definitions that stress a more dynamic view of equilibrium state that organizations are resilient if they can absorb stress while improving functionality (Hosseini *et al.*, 2016; Sheffi & Rice, 2005).

The improvement to organizational resilience is closely related to social resilience because an organization is a network of individuals who make up a business or industrial entity. Controls and administrative processes are how an organization controls resilience and minimizes the effects of adverse events or conditions(McManus *et al.*, 2008).

Industrial Process Resilience

Some industry sectors rely on assembly line type industrial processes that must be repeated several times in order to produce products at a massive scale. Resilience can be designed into these processes using ideas like robustness, redundancy, resourcefulness and rapidity (4R model) mentioned previously, to improve output and reduce risk associated with production. Industrial process resilience has been highly researched, and improvements have been implemented by industry to improve economic potential, as well as, the economy itself. In addition to Bruneau's (2003) 4R model for improving resiliency, Dinh *et al.* (2012) suggested six more factors that could improve resiliency in industrial processes. Dinh's six factors are: minimization of failure, limitation of effects, administrative controls and procedures, flexibility, controllability and early detection. Dinh's six factors incorporates the engineering principle of "graceful degradation" with organizational resilience and Bruneau's 4R model to provide a solid overall definition of industrial resilience from both the organizational and industrial process perspective (Bruneau *et al.*, 2003; Dinh *et al.*, 2012; Hosseini *et al.*, 2016).

International Business Machines (IBM) describes an organizational resilience framework that incorporates six "solution layers" that can improve an organizations resilience: strategy, organization, business and IT processes, data and applications, technology, facilities and security. This framework highlights the interdependencies in business processes and the information technology that supports those processes. The IBM strategy then goes on to define six resilience “building blocks”: recovery, hardening, redundancy, accessibility, diversification and autonomic computing. These building blocks are another term for dimensions of industrial resilience as defined by IBM (Goble *et al.*, 2002).

Chapter 3 will describe the various methodologies and frameworks for quantifying resilience. The chapter will also cover the various overall strategies for improving community and infrastructure resilience, as well as, conducting risk and vulnerability assessments. The chapter aims to make it clear that decision makers at all levels, along with infrastructure managers, would benefit from one single and unified methodology to quantify resilience, prioritize improvement projects, develop resilience strategy and assess the outcomes of implemented resilience strategy.

Chapter 3. Techniques to Model Resilience

Quantifying resilience is a challenge that academia and the U.S. Government have been researching to develop the best management strategies for infrastructure and community resilience. Quantifying resilience is difficult due to the many definitions and interpretations of resilience, and the number of models to describe and assess resilience are as numerous as those definitions. Each government agency is working on developing frameworks for assessing and identifying areas to improve infrastructure and community resilience, however the disjointed efforts are creating multiple frameworks that make resource allocation for infrastructure and community decision makers very difficult. If a community choses one agency's model or framework then the model used by another agency may not be fulfilled.

This chapter will review common models to quantify resilience in academia, as well as the frameworks for resilience assessment and infrastructure prioritization used by varying government agencies. While reviews of resilience assessment frameworks are common, this chapter will differ from most by considering vulnerability assessments or how infrastructure is targeted. By taking into consideration how an enemy may target infrastructure this chapter will identify knowledge gaps in current assessment frameworks that are not commonly considered. The purpose of this review will aid in identifying issues to be discussed in Chapter 4 to aid in developing a possible common framework to be used by infrastructure managers and community decision makers in the future.

COMMON MODELS FOR RESILIENCE

There are several ways to model resilience depending on the type and quantity of data available. Two general categories of models are qualitative and quantitative.

Qualitative models are those that assess resilience without using numerical descriptors. Qualitative models are typically conceptual, empirical, or semi-quantitative. Conceptual frameworks make up a majority of the qualitative frameworks and describe best practices for resiliency. Semi-quantitative models are assessments of qualitative aspects of resilience (Hosseini *et al.*, 2016).

Quantitative models consist of general resilience approaches that measure resilience across a wide range of applications and structural based approaches. Structural based approaches model network specific approaches to the components of resilience (Hosseini *et al.*, 2016). General approaches can be either deterministic or probabilistic. A deterministic approach does not consider uncertainty or the probability of a disruption, while a probabilistic approach takes randomness and irregularity or stochasticity, inherent in an infrastructure system into account. Another consideration is the temporal aspect of resiliency. Dynamic models account for time dependent reactions while static models are independent of time. Structural based approaches can be seen as an optimization model, a simulation model, or a fuzzy logic model. Optimization models attempt to maximize resilience of a network by designing in metrics to limit disruptions and cascading effects of disruptions. Simulation approaches model a network and simulate different events iteratively to maximize resilience of a network. Fuzzy logic models are used in organizational resilience to interpret linguistic variables into quantitative variables or measures for resilience (Aleksić *et al.*, 2013; Hosseini *et al.*, 2016).

One of the most common general deterministic models for resilience was introduced by Bruneau *et al.* (2003) that defined a resilient system as one that displayed reduced failure probabilities, reduced consequences from failures in terms of lives lost, damage, negative social and economic outcomes and a reduced time to recovery. Bruneau's definition looks at resilience from an engineering perspective where resiliency has a single state of equilibrium or normalcy. Bruneau *et al*. (2003) also describes four dimensions of resiliency that are commonly found throughout literature. The dimensions are robustness, redundancy, resourcefulness and rapidity. Robustness, refers to the strength or ability of a system to withstand stress or a demand without suffering degradation. Redundancy, is the extent to which a system is sustainable or capable of fulfilling its requirements in the event of a disruption, degradation or loss of functionality. Resourcefulness, is the capacity to identify problems, establish priorities and mobilize resources in the event of a disruption. Resourcefulness can also be seen as the ability of a system to apply material and human resources to meet establish priorities and achieve goals. Rapidity, is the capacity to achieve goals and meet priorities in a timely manner so as to contain losses and avoid further disruption (Bruneau *et al.*, 2003). Bruneau, working in conjunction with the Multidisciplinary Center for Earthquake Engineering Research (MCEER), introduced the resiliency triangle depicted in figure 2 in order to model his definition and depict a graphical measure of resiliency, where the characterization of the system functionality at a given point is defined by the attributes of robustness, redundancy, resourcefulness and rapidity. It's the combination of the four attributes listed above that leads to the Resilience Triangle for Civil Engineering (Bruneau *et al.*, 2003). The quality of service provided by the system is modeled on the vertical axis and time is depicted on the horizontal axis. The measure of resilience is then the area in the triangle, or the disrupted portion of the line.

Figure 2 below, depicts the MCEER resiliency triangle developed by Bruneau *et al.* (2003). The quality of infrastructure, Q(t), varies with time and is the quality of service delivered to a community from a particular piece of infrastructure. Performance can be from 0 percent to 100 percent, where 100 percent is full services provided with no disruptions and 0 percent means no service is provided. If a disruption occurs at time t_0, the disruption may cause damage to the infrastructure and reduce the quality of service (Figure 2 shows a disruption from 100 percent to 50 percent). Time t_1 in Figure 2 depicts when the infrastructure is restored to the point where it can provide full services again. The loss in resilience, R, is the area under the service line between t_0 and t_1 and can be defined mathematically with the equation as follows (Bruneau *et al.*, 2003):

$$R=\int_{t_0}^{t_1}[100-Q(t)]dt$$

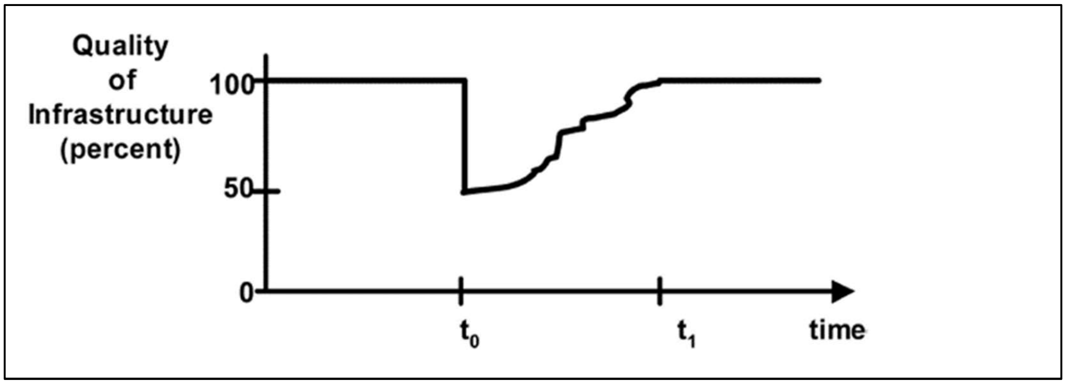


Figure 2: The MCEER resiliency triangle (Bruneau *et al.*, 2003).

Another model used to simulate and describe the cascading effects of disruptive events on an infrastructure system is the input-output agent-based model. Olivia *et al.* (2010) introduced an input-output agent-based model to identify and understand the global weaknesses of highly complex infrastructure systems and their components. The agent-based input output model proposed by Olivia *et al.* (Olivia *et al.*, 2010) described infrastructure interdependencies by decomposing infrastructure networks into a series of interconnected elements producing and consuming resources while taking into consideration the transmission of goods and services between the elements. Agent based models are used to describe bi-directional networks. In other words, networks in which the different elements or entities in the network are interconnected and reliant on the other elements in the network to receive and produce goods and services. Modern infrastructure systems are not only bidirectional, but they are also highly interdependent and heterogeneous and can be considered as edge-weighted bidirectional graphs (Barrat *et al.*, 2004; Haimes & Jiang, 2001). The weight of links within infrastructure systems represent the degree of dependency of the resource or service, and the direction of the links indicates the direction of the link's flow.

Modeling and characterizing bidirectional systems is often accomplished using network theory as a tool. Network theory transforms major components within the bidirectional system into nodes and the dependencies between the nodes into links (Dunn *et al.*, 2013; Patterson & Apostolakis, 2007; Svendsen & Wolthusen, 2007). Once the nodes and links are identified within the infrastructure system they can be ranked or sorted according to any parameters specified (Sun & Han, 2014). Network theory offers a wide range of parameters to rank or prioritize nodes and links. Network theory is used to model real world problems involving physical-, biological-, social-, economic- and information systems. For example, in economic systems, node ranking is used to study the patterns in international trade to identify strong and weak economic centers (Fagiolo *et al.*, 2010). Node ranking in physical infrastructure has a number of applications for different parts of infrastructure systems such as electrical grids, water distribution networks, etc. (Wang *et al.*, 2010). In infrastructure networks, ranking of nodes is required to identify the components which are most critical in terms of performance and security of the entire network.

Determining the components that are most critical can be achieved by determining centrality metrics. To determine the degree of centrality there are four metrics: 1) degree of centrality, 2) closeness centrality, 3) betweenness centrality 4) eigenvector centrality. The degree of centrality is a measure of the total number of incoming and outgoing connections from a given node to other nodes in the network. Closeness centrality is the measure of how close a node is to the other nodes in a network. Betweenness centrality is the measure of how close to the center of a network a node lies in space or importance. Finally, eigenvector centrality is a measure of importance based on its connection to other high priority nodes in the network. Centrality metrics can be used when determining which nodes are more critical for the overall operation of the network as a whole (Li *et al.*, 2015). Models for simulating and optimizing infrastructure resilience can be based on time, as well as, being based on the topology or layout of the network. Both methods have advantages and disadvantages. Some networks, such as electrical grids or water distribution networks are modeled based on time, while other networks are characterized by the layout of the network with respect to the topology of the area (Panteli & Mancarella, 2015).

Ting (2003) introduced a game-theory model to assess the redundancy in bureaucratic arrangements in order to assess whether redundant bureaucracy in government is a wasteful duplication of efforts, or a measure to create resiliency against political uncertainty. Prior to Ting's work, strategic issues in governance like collective action issues or competition were ignored. Ting (2003) introduced his game theory model of government policy making in which a political principle chooses a number of agents to handle a task. Each agent chosen has policy preferences that may or may not be opposed to the political principals and each agent can also choose different policy or effort levels. Results from the model showed that redundancy in government can help a political principle achieve its goals when preferences are not aligned with the agents. The redundancy is less effective when different agents' preferences are all closely aligned to the principals. In the game theory environment where preferences are closely aligned, collective action problems cause multiple agents to be less effective than a single agent. In addition, if the agents that enact policy changes can be overruled then redundancy in effort is unnecessary. The model proposed by Ting (2003) shows that the efforts for resiliency conducted by multiple federal agencies are somewhat redundant and unnecessary, supporting the conclusion that a single entity that has jurisdiction over resiliency should be chosen since community resilience has become viewed as a necessary component of local governance (Ting, 2003).

COMMON FRAMEWORKS USED TO ASSESS RESILIENCE

It is common for federal agencies, academia, infrastructure managers and community decision makers to develop and adopt frameworks for assessing resilience based on the models available from academia in an attempt to optimize resources used to improve resilience. In the DOD, it is common to consider infrastructure as a viable military target when considering the best means of pacifying a threat community or region. Typically, military plans involve disrupting infrastructure while causing the least amount of damage in order to achieve an objective while maintaining the ability to restore the infrastructures services or functionality once the threat is removed. Rarely are targeting frameworks compared to vulnerability assessment frameworks to determine the optimum resource allocation to achieve resilience. This chapter will look at frameworks used to improve resilience, along with frameworks used to target infrastructure, in an attempt to identify knowledge gaps or consideration gaps not commonly discussed.

The DHS created the National Infrastructure Protection Plan (NIPP) to address the need for a framework to quantify resilience. The NIPP, however, does not drive coordinated resiliency work, where each office within the DHS approaches resiliency frameworks differently. The DHS office of health affairs is creating a "Community Health Resilience Guide" that is meant to provide a framework for practitioners and policymakers to assess and improve community health resilience from a system-wide perspective. The guide does not, however, quantify the checks involved in the framework to develop a resiliency score. The Federal Emergency Management Agency (FEMA) is responsible for disaster response and recovery and is therefore critical to community resilience plans. FEMA is developing a certification program that outlines pre- and post-disaster checklists for specific stakeholders. Frameworks used by FEMA include the National Disaster Recovery Framework (2010), and the Whole Community Approach to Emergency Management (2011) (Aldrich & Meyer, 2015). The DHS Office for Cyber Security and Communications provides a software tool that allows organizations to assess their information technology network compared to industry standard security practices. The cyber tool can be used to determine recommendations for improving cyber security but is focused on the pre-disaster resilience phase. The Office of Infrastructure Protection conducts a resilience audit known as the Regional Resiliency Assessment Program (RRAP). The RRAP assesses the preparedness and protection capabilities of the critical infrastructure owners, law enforcement and emergency response organizations. The RRAP then provides findings to identify investments for the improvement of critical infrastructure resilience. The DHS Science and Technology Directorate conducts social and behavioral research to improve communication and guidance to improve community resilience (Larkin *et al.*, 2015).

The Department of Interior (DOI) Metric Expert Group (DMEG) was initiated within the Watershed Research Group of the United States Geological Survey (USGS) after Hurricane Sandy to address the challenges associated with improving costal resilience. The DOI accomplishes this by restoring federal assets, increasing the ability of a community to absorb damage from a hurricane and improve maintenance on the coastal resource system. DMEG is responsible for assessing the effectiveness of DOI resilience programs by providing a review that resulted in a summary of resiliency efforts, knowledge gaps, shortcomings and a list of things that need to be resolved in order to optimize management practices in providing resiliency (Larkin *et al.*, 2015).

The Environmental Protection Agency (EPA) defines resilience as "the capacity for a system to survive, adapt and flourish in the face of turbulent change." The EPA manages resilience by utilizing varying methods to quantify and monitor disruptive changes in the economic, environmental and social systems of a community. The EPA is therefore concerned with increasing preparedness for systems exposed to an external shock. The EPA uses adaptability, cohesion, latitude and resistance as metrics to measure resilience. Adaptability is the ability of a system to change in response to changing pressures. Cohesion is the strength of the bonds between different elements of a system. Latitude is defined as the maximum amount of change a system can withstand. Finally, resistance is the ability of a system to stay the same when faced with disruption. The EPA uses qualitative methods to measure community resilience when quantitative data is not available. The EPA views their assessment method as a first look at how to reduce risk that a system faces while taking a first step toward improving resilience. The EPA does have some programs, like the Gulf of Mexico Program, which is helping coastal communities to identify risks and promote overall community resilience to hazardous events (Larkin *et al.*, 2015).

A subdivision of the National Institute of Standards and Technology (NIST) called the Materials and Structural Systems Division focuses on enhancements in building materials and physical infrastructure and is responsible for developing NISTs Disaster Resilience Framework. The Disaster Resilience Framework (DRF) is designed to improve the resilience of community infrastructure against natural and man-made physical disasters. Natural disasters are severe storms and other natural hazards, while man-made physical disasters are accidents or attacks such as blasts, or vehicle impacts. The DRF provides community decision makers with performance measures with respect to time, and strategies to improve resilience before, during and after an event. NIST defines three stages of recovery that support absorption, recovery and adaptation. The three stages are the response stage, the workforce recovery stage and the community recovery stage. The *"response stage,"* occurs immediately after the event and lasts for three days. The main focus of the response stage is providing critical aid for the community before and during an emergency. NIST defines critical aid as aid which assists with life safety, food and water resources, shelter, health and situational awareness. The *"workforce recovery stage*," starts after the response stage and ends twelve weeks after the incident. The workforce stage addresses performance objectives that help a community recover quickly and effectively. The community recovery stage starts four months after the event and can last upwards to 36 months. The "*community recovery,*" stage involves projects that are concerned with the long-term reconstruction of the community that allows for growth and future resilience (Larkin *et al.*, 2015).

The National Oceanic and Atmospheric Administration provides decision makers with the most up-to-date information on climatic areas of research like weather forecasts, climate monitoring and coastal restoration. NOAA assists communities in evaluating the degree to which they are prepared for coastal storms by providing a Community Resilience Index. The Community Resilience Index has six parts with a series of "yes" or "no" questions, each representing a distinct indicator of resilience. Community leaders can then count the checkmarks to determine if their community is resilient based on a "Low," "Medium," or "High" score. The Community Resilience Index is meant as a tool to identify weaknesses in current coastal communities and provide a discussion point for improving resiliency plans. Another resilience tool developed by NOAA is the "Port Tomorrow: Resilience Planning Tool," which offers points of consideration for marine transportation project development or assessment (Larkin *et al.*, 2015).

The DOD is interested in resilience of not only infrastructure, but also its equipment and service members. Two entities within the DOD that look at infrastructure and community resilience within the U.S. are the U.S. Army Corps of Engineers (USACE) and the U.S. Army Environmental Command (USAEC). USACE is primarily responsible for the management of federal waterways, but also has a responsibility to aid in disaster management. The Coastal Engineering Research Board (CERB), which falls under USACE, developed a three-tiered methodology for assessing coastal communities for both short term resilience to specific hazards and long-term resilience to changes in population dynamics and changes in climate. This three-tiered methodology will be used by USACE to plan, design and assess coastal region resilience. Tier 1 assesses the overall coastal community resilience and defines effectiveness of physical infrastructure in terms of community behavior (evacuation), values (economy), knowledge (understanding of risk), and governance (building codes, emergency management). Tier 1 prioritizes projects that provide the greatest increase in resilience across the most components of the system. Tier 2 is an assessment of the community, ecological and engineered coastal protection structures. Tier 2 uses the NOAA Community Resilience Index as a tool and aims to quantify resilience of the existing infrastructure. Tier 3 develops a model of physical infrastructure and is evaluated under various simulated disturbances to develop an understanding of expected performance. USACE has also developed a resilience assessment scorecard for all USACE projects beyond coastal protection (The US Army Corps of Engineers, 2016; Larkin *et al.*, 2015).

USAEC has developed a Military Installation Resilience Assessment (MIRA) for all threats faced by U.S. Army installations. The assessment considers both socio-ecological and engineering resilience. The MIRA is both a hazard specific risk assessment as well as a scenario-based tool for assessing altered states after a hazard has occurred. MIRA also can be used to identify dependencies and feedback loops of different system components, analyze stakeholder involvement and determine the cost effectiveness of potential solutions. Final resiliency scores of the MIRA are on a 1-7 scale based on comparison of assessed criteria. MIRA is designed to provide a consistent method for installation managers to assess resilience of their facilities and make decisions related to resilience of both mission critical systems and facilities (Larkin *et al.*, 2015).

Other agencies within the federal government are contributing to resilience efforts but have not yet developed a framework for assessing and improving resilience. Federal agencies have begun collaborating with each other and with outside organizations to develop further resilience tools. An example of collaboration is the Resilience Integrated Action Team (IAT) which was established as a federal cabinet-level inter-department committee chaired by the NOAA and USACE. IAT consists of members of over fifteen agencies and is developing frameworks for managing the Marine Transportation System. The Argonne National Laboratory is developing a resilience assessment framework discussed in this thesis based on the RRAPs model for community resilience and has provided support to DHS's Enhanced Critical Infrastructure Protection Program. NIST has also funded Bruneau at the University of Buffalo to complete his PEOPLES resilience framework (Larkin *et al.*, 2015; Renschler *et al.*, 2010) . The Department of Health and Human Services (DHHS) has a strategic planning framework designed to enhance the security of the United States in times of crisis called the National Health Security Strategy (NHSS) (Aldrich & Meyer, 2015).

Schroder et. al. (2012) introduced a framework for prioritizing infrastructure improvements on critical freight corridors that acknowledged the limited budget faced by state governments. The framework uses an input-output model to produce a prioritized list of infrastructure needs based on economic metrics compared to infrastructure performance and level of service. The developed decision model, metrics and prioritization framework are designed to be applicable to any region within the United States. The performance measures used by Schroder *et al.* (2012) are based on the National Bridge Investment Analysis System (NBIAS), the International Roughness Index (IRI) and truck crash rates. This model is good for transportation infrastructure, such as highways and bridges (Schroeder *et al.*, 2012). Other international frameworks for resilience include The United Nations Making Cities Resilient Campaign (Aldrich & Meyer, 2015; Pagano *et al.*, 2018).

Assessing Resilience

The DHS has funded the Argonne National Laboratory to develop a Resilience Index (RI) to assess resilience of critical infrastructure systems as defined by the National Infrastructure Protection Program and the Enhanced Critical Infrastructure Protection (ECIP) program. The RI methodology considers all parts of critical infrastructure systems with respect to resilience from threats and threat consequences. The RI is intended to generate reproducible results to support risk management decision making, disaster response and business continuity (Fisher *et al.*, 2010). The data used in developing the RI was collected through a modified ECIP program and is derived from robustness, resourcefulness and recovery categories. The RI ranges from 0 (low resilience) to 100 (high resilience) but is not indicative of whether or not an event will affect a facility or if an event will cause severe consequences. The RI is instead used to compare resilience at critical infrastructures to guide decisions on prioritization of resources to improve resilience. The RI is combined with other indices like the vulnerability index, the protective measures index and the criticality index to support decision making regarding risk, protection, business continuity and emergency management (Fisher *et al.*, 2010). The DHS RI is developed in conjunction with the DHS Regional Resiliency Assessment Program (RRAP). The RRAP is a voluntary program to assess critical infrastructure in a geographic area combined with a regional analysis of infrastructure to determine a wide range of infrastructure issues that may have consequences at the regional and national level. The goal of RRAP is to develop the understanding of and the actions required to improve a region's resilience by both public and private entities. The RRAP resolves security issues and resilience knowledge gaps, aids with risk management decisions, identifies opportunities and strategies to improve infrastructure resilience. It improves partnerships between public and private stakeholders to achieve its overall goal of improving regional resilience (The Department of Homeland Security, 2009).

The NIST has funded Bruneau at the University of Buffalo to develop his PEOPLES resiliency framework (Larkin *et al.*, 2015). PEOPLES is an acronym for the seven dimensions of community resilience as defined by Bruneau. The seven dimensions are: Population and demographics, Environmental/Ecosystem, Organized Governmental Services, Physical Infrastructure, Lifestyle and Community Competence, Economic Development and Social-Cultural Capital. The framework provides the basis for qualitative and quantitative models to constantly measure resilience of communities to extreme events in any single dimension or combination of dimensions in the PEOPLES framework. The framework expands on Bruneau's previous research with the Multidisciplinary Center for Earthquake Engineering Research (MCEER) by linking the 4 R's of resilience (robustness, redundancy, resourcefulness and rapidity) to the resilience dimensions (technical, organizational, societal and engineering) to produce a disaster resilience measure for different types of assets in an infrastructure system (Renschler *et al.*, 2010). A similar model that denotes a community-based, holistic and scalable approach to resilience was developed by Longstaff *et al.* (2010). The Longstaff *et al.* (2010) framework for community resilience focused on five key community subsystems as opposed to seven: 1) Ecological, 2) Economic, 3) Civil Society, 4) Governance and 5) Physical Infrastructure (Longstaff *et al.*, 2010).

Francis and Bekera (2013) developed a framework focused on improving the adaptive capacity, the absorptive capacity and recoverability in infrastructure systems. Francis and Bekera's framework consist of four stages; 1) system identification, 2) objective setting, 3) vulnerability analysis, 4) stakeholder engagement. The framework proposed is theoretical in nature and provides insight into the issues faced with resiliency research. The framework proposed provides a good knowledge base for resiliency research and analysis, but would require the backing of a federal agency to be put into operation. Argonne's RI and Bruneau's PEOPLES frameworks are more likely to be used because of their backing by DHS and NIST respectively (Francis & Bekera, 2014).

Ouyang *et al.* (2012) also introduced a framework to address the capability of infrastructure to resist any hazards, absorb initial damage and recover to the functionality of normal operations or improve to a new level of operation. The framework proposed by Ouyang *et al.* (2012) is a three-stage framework. Stage one is the disaster prevention stage that demonstrates the resistance capability of a system to prevent any possible hazards and limit initial damage from any hazard occurrence. Stage two indices of "hazard frequency" and "initial damage level" describe the resistance capacity of a system. The first stage mainly focuses on local level impacts relating hazards to component level failures. The second stage is the damage propagation after initial hazards. The second stage shows the absorptive capacity of a system as the ability of a system to withstand initial damage and minimize the propagation of failures or cascading failures. The second stage focuses on system-level failures and translates initial local component failures into system level consequences. The third stage is the recovery process where damage information is collected and resources are allocated to restore performance. The third stage focuses on restoration response translating external response into system recuperation. System resilience can be improved during any one of the three stages (Ouyang *et al.*, 2012).

Cutter *et al.* (2008) developed an assessment framework called Disaster Resilience of Place (DROP). The DROP model was designed as a quantifiable means to present the relationship between vulnerability and resilience that can be readily applied to real problems in real places. The DROP model considers the pre-existing conditions in a community prior to a disaster or hazard conditions. Unlike other models discussed, this model considers hazard severity, the hazard frequency and pre-existing conditions in the community (resources available) (Cutter *et al.*, 2008).

Assessing Vulnerability

Another angle to approach a community's resilience is to look at a community from the vulnerability aspect. The military and the government often look at communities from the perspective of targeting in order to gain a military advantage or to stabilize a community under the threat of insurgent forces attempting to destabilize a region and assert control over a community. Understanding frameworks for targeting infrastructure and conducting criticality assessments (from the targeting perspective) provides insight into what areas need to be protected from not only man-made hazards, but also natural hazards. Natural hazards and manmade hazards both have the ability to create failures that can propagate throughout a system or a community.

When approaching the problem of stabilizing a nation such as Iraq and Afghanistan, the Department of Defense developed a methodology and framework to define external environment problems in an effort to develop better strategies. The methodology and framework considers Political, Military, Economic, Social, Information, Infrastructure, Physical Environment and Time (PMESII-PT) aspects of a society or region. This framework is easily adjusted to commercial aspects of a community in the U.S. by exchanging the military aspect for the competitors in the business world.

Another strategic planning tool closely related to PMESII-PT and used by the commercial industry is STEEPLE or Social, Technological, Environment, Economic, Political, Legal and Ethical. Both frameworks can be used to anticipate future impacts of decisions and anticipate future trends based on the macro or external environment. These analysis tools can aid in determining which factors will influence the community in the future. For this thesis, the PMESSII-PT will be the focus due to the fact that the two models are very similar, and that the military plays a key role in disaster response and recovery (Walden, 2011). This framework can be readily applied to any community and is all encompassing. The focus of the assessment can be adjusted to resiliency and some terms like "military" can be adjusted to be more fitting (IE law enforcement or first responders), but that is an easy adjustment to an assessment framework that has been demonstrated as useful to nation building efforts conducted in the past.

Political and Military aspects of PMESII-PT are clearly defined by the DOD. The political environment describes "the distribution of responsibility and power at all levels of governance" (DOA / US, 2017). The military aspect of the external environment is defined as "the military capabilities of all armed forces in a given operational environment. For many states, an army is the military force primarily responsible for maintaining internal and external security" (DOA / US, 2017). Both of these aspects are crucial to the recovery aspect of resilience and can be used to describe both the resourcefulness and rapidity of a community's recovery capabilities. The community's ability to police itself (including jail cells available) after a disaster (keeping in mind that the police are affected by the disaster as well) or the state's ability to provide National Guard assets are key components of resiliency.

The economic aspect of a community's environment is defined in the military as "individual and group behaviors related to producing, distributing and consuming resources" (DOA / US, 2017). The economic aspect is extremely important to determining the resources required to respond to a community, or the resources that are available to a community to deal with natural hazards. This aspect also covers the regional and national level implications of economic failures in a particular community.

The military defines society as "a population whose members are subject to the same political authority, occupy a common territory, have a common culture, and share a sense of identity" (DOA / US, 2017). It is important to consider society in resilience planning because their inherent characteristics can determine if one community is more resilient than another based on demographics like those listed above.

Information in the community environment can be defined as "the aggregate of individuals, organizations and systems that collect, process, disseminate, or act on information" (The Joint Chiefs of Staff, 2014) (Walden, 2011). Citizens of a typical U.S. community rely on several means of information gathering including smart phones, landlines, internet, TV, Radio and newspapers. In fact, there are so many forms of communication that oftentimes may be difficult to decide which medium is best for reaching the population effectively. Planning and preparing for disaster response are a critical aspect of disaster resilience and how to disseminate information is a key aspect of planning that community decision makers must consider. Conversely, how emergency responders and community leaders coordinate and communicate before, during and after hazards must be taken into consideration.

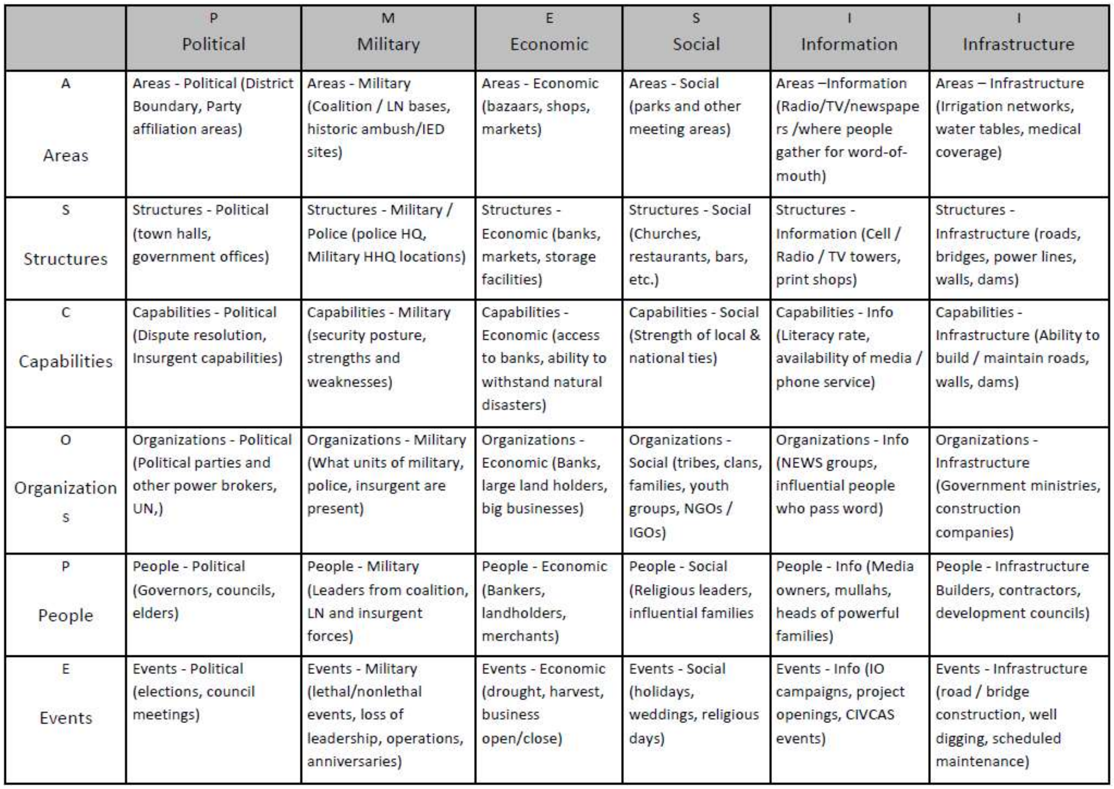
Infrastructure in military terms is the same as in engineering terms and looks at road networks, pipelines, energy grids, wastewater and water treatment, water distribution networks, etc. Critical infrastructure is the subject of the rest of this thesis and is included in this aspect. Other things to consider with infrastructure is how it will respond under hazardous conditions. For example, how will a road network handle a mass evacuation?

Will there be enough fuel and maintenance equipment along the route to handle increased volume? These are the types of considerations considered in this aspect as well.

Physical Environment in the military is defined as, “the geography and manmade structures” (DOA / US, 2017). This definition considers that bridges and buildings can create corridors for movement or physical barriers. The military is concerned by buildings because it makes a combat zone have a more 3D aspect with multiple levels. For resilience the concept of physical environment can describe how runoff will affect flood zones, or how proximity to a river or coastline can affect a city. For instance, evacuation routes can be planned to avoid routes that cross floodplains or are reliant on one single bridge or piece of infrastructure that is itself threatened.

Time to the military is the amount of time available to prepare for an operation, to conduct an operation and how long can an enemy conduct prolonged combat. Time can be seen from the lens of resiliency as well. How long does it take to evacuate? When does an evacuation order need to be issued? How long does it take to prepare a city for a hurricane? How long do typical storms last? and other similar considerations in terms of time can be applied to community resilience. Time to recover different pieces of infrastructure can be applied to resilience assessment as well. Consideration for second and third order effects of infrastructure downtime should be made. For example: If the power goes off how long until milk or produce goes bad? How long until hospitals need to be evacuated? Understanding the implications of infrastructure downtime can inform community disaster planners on how to sequence local, state and federal aid.

The PMESII-PT construct is also often times assessed from six different civil considerations to create a crosswalk that planners can use to cover every aspect of an environment and society. The six considerations are: Area, Structures, Capabilities, Organizations, People and Events (ASCOPE). For example the political aspect of PMESII-PT is analyzed by political areas (congressional districts, political boundaries), political structures (government buildings), political capabilities (dispute resolution, ability to execute orders), Political organizations (political parties, power brokers), political people (congressmen, representatives, mayors, etc.) and political events (elections, city council meetings, rallys, etc.) (US Marines, 2019). An example ASCOPE to PMESII crosswalk is provided in Table 1.



	P Political	M Military	E Economic	S Social	I Information	I Infrastructure
A Areas	Areas - Political (District Boundary, Party affiliation areas)	Areas - Military (Coalition / LN bases, historic ambush/IED sites)	Areas - Economic (bazaars, shops, markets)	Areas - Social (parks and other meeting areas)	Areas –Information (Radio/TV/newspapers /where people gather for word-of-mouth)	Areas – Infrastructure (Irrigation networks, water tables, medical coverage)
S Structures	Structures - Political (town halls, government offices)	Structures - Military / Police (police HQ, Military HHQ locations)	Structures - Economic (banks, markets, storage facilities)	Structures - Social (Churches, restaurants, bars, etc.)	Structures - Information (Cell / Radio / TV towers, print shops)	Structures - Infrastructure (roads, bridges, power lines, walls, dams)
C Capabilities	Capabilities - Political (Dispute resolution, Insurgent capabilities)	Capabilities - Military (security posture, strengths and weaknesses)	Capabilities - Economic (access to banks, ability to withstand natural disasters)	Capabilities - Social (Strength of local & national ties)	Capabilities - Info (Literacy rate, availability of media / phone service)	Capabilities - Infrastructure (Ability to build / maintain roads, walls, dams)
O Organizations	Organizations - Political (Political parties and other power brokers, UN,)	Organizations - Military (What units of military, police, insurgent are present)	Organizations - Economic (Banks, large land holders, big businesses)	Organizations - Social (tribes, clans, families, youth groups, NGOs / IGOs)	Organizations - Info (NEWS groups, influential people who pass word)	Organizations - Infrastructure (Government ministries, construction companies)
P People	People - Political (Governors, councils, elders)	People - Military (Leaders from coalition, LN and insurgent forces)	People - Economic (Bankers, landholders, merchants)	People - Social (Religious leaders, influential families	People - Info (Media owners, mullahs, heads of powerful families)	People - Infrastructure Builders, contractors, development councils)
E Events	Events - Political (elections, council meetings)	Events - Military (lethal/nonlethal events, loss of leadership, operations, anniversaries)	Events - Economic (drought, harvest, business open/close)	Events - Social (holidays, weddings, religious days)	Events - Info (IO campaigns, project openings, CIVCAS events)	Events - Infrastructure (road / bridge construction, well digging, scheduled maintenance)

Table 1: PEMESII-PT and ASCOPE crosswalk (US Marines, 2019).

In addition to the PEMESII-PT and ASCOPE crosswalk the government already has a tool for assessing the interrelationships between assets, threats, vulnerabilities and countermeasures to protect a facility. The Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability (CARVER) matrix was developed by the Special Forces in Vietnam to rate the relative desirability of targets for the allocation of attack resources. Today, the DHS, the USFDA (U.S. Food and Drug Administration), the DOD, and some state and local governments use variants of this tool to reverse engineer hazards to determine the allocation of resources to protect or assess the vulnerability of community assets such as infrastructure. The CARVER tool is limited in that it is somewhat subjective and qualitative in nature and needs replacement by a quantitative tool that can be consistently replicated.

As defined earlier, CARVER stands for Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability. Criticality is the importance of a system, subsystem, complex, or component. Something is critical when its destruction or damage has a significant impact on the output of the system, subsystem, or complex. A hazard disrupting a critical piece of infrastructure would significantly impair or damage political, economic, and government operations, or civil society. Criticality can be impacted by time, quantity or quality of the service disrupted and the ability to replace the component. Accessibility is the ease at which a system or component can be reached by a hazard, either natural or manmade. Recuperability is how long it would take to repair, replace, bypass, or restore a system or component. If the system or component is cheap and easy to repair, then it is less likely to be a terrorist target or become a major issue during a natural hazard. Vulnerability is the level of protection or exposure to either manmade or natural hazards. The effect is the scope and magnitude of adverse consequences that would result from any disruption. Recognizability is the degree to which a system or component can be recognized without confusion. Recognizability applies more to manmade hazards than natural hazards which do not discriminate based on physical appearance. Each component of a system is given a score based on a pre-determined rubric to determine which components or sub-components are most vulnerable. The USFDA uses a tool known as CARVER+Shock. The CARVER+Shock tool uses all of the same criteria briefly discussed earlier but adds Shock or the psychological effect of a successful attack or degradation would have on the population affected. The CARVER method uses metrics for each of the criteria to determine a number value for each criteria. The totals are then added to determine which systems or components are more critical than others. The USFDA has a standard metric used to assign a number to each of the criteria (Bennett, 2007).

A similar tool used by the DOD is the DSHARPP matrix which assesses vulnerability in the same way as the CARVER matrix, only using Demography (Who is being targeted? Are the inhabitants or targets part of a larger organization?), Symbolism, History, Accessibility, Recognizability, Population and Proximity (proximity to other targets of higher significance) as the criteria measured. Local and state governments sometimes replace the Demography with Mission or the mission of the asset in question to create a similar vulnerability matrix known as the Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity (MSHARPP) matrix (Bennett, 2007).

PRIORITIZING INFRASTRUCTURE RESILIENCY IMPROVEMENT PROJECTS

The goal of the frameworks described above are to identify weaknesses and vulnerabilities in infrastructure and the community. Once the vulnerabilities and weaknesses are identified decision makers must then allocate their limited resources to meet the objectives they have for the community. Assuming that a community's objective was resilience, priorities would need to be set in order to optimize infrastructure resilience in a timely manner. Even if there were unlimited resources it is unlikely that a community would be able to protect itself from all threats that it could face (Larkin *et al.*, 2015; Longstaff *et al.*, 2010). The complexities within infrastructure systems that support modern life tend to reduce resilience through a loss in redundancy and diversity and are typically not designed with resiliency as a specification (Longstaff *et al.*, 2010). In order for community decision makers to make repeatable decisions with respect to resilience that will survive political turnover, quantifiable means of prioritizing infrastructure for resources need to be established.

Recently, there has been interest in researching methods to prioritize infrastructure given limited resources. This section will provide a list of some methods used to prioritize infrastructure for community decision makers. While these are some ways to prioritize infrastructure for resilience, a unified method that can be applied to communities is still in need of being researched and applied universally in order to improve national resilience.

In order to prioritize infrastructure for repair or resiliency improvements community decision makers should look at infrastructure from a perspective of asset management. In asset management, levels of expected service must be developed in order to make prioritization decisions. The concept of Levels of Service (LOS) has been used for highways since the mid-60s but can be employed on other infrastructure systems. LOS is the qualitative measure of expected operating conditions on a highway and is typically measured in terms of traffic speed, travel time, maneuverability, etc. Other infrastructure systems use Maintenance Quality Assurance (MQA) as a measure of the level of service expected from a given infrastructure system. The American Society of Civil Engineers (ASCE) and the Washington State Department of Transportation use an “A” through “F” scale. “A” denoting a high level of service and “F” denoting a poor level of service provided to the customer. The “customer” in infrastructure is typically the citizens or businesses relying on the infrastructure daily. They can be considered the “customer” because they are the taxpayers who fund most infrastructure services. The goal of infrastructure is to meet the customer demands and those demands should be taken into consideration when making prioritization decisions (Bolar *et al.*, 2017).

One method, used in manufacturing, that can be used to involve the customer requirements in the decision-making process is called the Quality Function Deployment (QFD). QFD is popular within the automotive industry and the aerospace industry, but can be applied to infrastructure like power grids and water treatment/distribution networks in terms of meeting the demands of the customers or community. Communities can utilize the QFD in order to identify customer requirements over time to provide the data necessary upon which to base infrastructure resilience and improvement decisions (Bolar *et al.*, 2017).

Infrastructure prioritization is typically conducted on a project by project level. One of the commonly used models for project prioritization is based on cost-benefit analysis (CBA). CBA is typically based on a single metric with monetary value for a project. CBA looks at all of the present and future costs and places them in terms of present value. This single value allows decision makers to rank diverse projects on a single metric. Another form of CBA is the social cost benefit analysis (SCBA). SCBA allows decision makers to prioritize projects that maximize the net present values for society as a whole. The issue incorporating SCBA lies in the fact that it requires a large amount of information and requires applying a quantifiable value to reflect positive and negative effects of a project. SCBA is expensive and time consuming and is therefore not feasible for all projects.

Another newer method for prioritizing infrastructure projects is the Multi-Criteria Decision Analysis (MCDA). The MCDA decision models formalize the inclusion of non-monetary and qualitative factors into the decision-making process when information or analytical resources are limited (social capital, for example). MCDA relies on federal agency or organizational policy to select and weigh criteria to assess alternatives (Marcelo, Mandri-Perrott, House, & Schwartz, 2016).

Another method for infrastructure prioritization is part of the World Bank Unified Framework on Public Infrastructure Management (PIM). The PIM is intended to help government agencies through the process of infrastructure investment and delivery effectively and efficiently. The World Bank recognizes that infrastructure prioritization is important when there are resource constraints, and therefore The World Bank developed the Infrastructure Prioritization Framework (IPF). The IPF is a quantitative multi-criteria approach that incorporates financial, economic, social and environmental conditions. All of the criteria are categorized into two indices or the social-environmental index or the financial-economic index. The indices are then considered in terms of the budget constraint for a particular sector. Unlike other decision tools, IPF incorporates policy goals, social and environmental sustainability, as well as long-term development goals. The IPF displays results graphically to provide decision makers with the ability to easily compare alternative investment scenarios. (Marcelo *et al.*, 2016).

Strategies for Improving Resilience

Regardless of the asset management and resilience project prioritization framework chosen, an overall resilience strategy must first be established to determine the criteria by which resiliency improvement projects are evaluated. Yodo and Wang (2016) argue that there are two essential resilience attributes: reliability and recovery, that must be part of an engineered system in order for it to be considered resilient. Infrastructure systems need an improved ability to recover and have improved reliability designed into the system. Reliability can be generally defined as: the probability that a system will perform as required for a specified period under designated operating conditions. Tools like the reliability-based design optimization framework and the effective reliability analysis methods for design can be used to improve reliability during the design phase of a project. Since all hazards and failure modes cannot be taken into consideration during the design phase, derating and diversity are design techniques that can be incorporated to improve reliability. Derating is using higher tolerance components that provide more endurance then normally required. Diversity is having multiple sources of resources required by a component available to ensure reliability of supply. Another strategy for improving reliability is improving failure diagnosis, improving the prognosis and health management (PHM) process, and improving the operation and maintenance plans. Improving monitoring and maintenance strategies limits the amount of time a system operates at degraded levels and therefore improves the system's ability to withstand change (Yodo & Wang, 2016).

In many instances a swift recovery depends on the amount of resources (material and personnel) readily available to repair or replace a damaged component, as well as, the time it takes to replace those components. Resourcefulness, or a high level of preparedness along with collaboration and a good resource allocation strategy can be designed into a system to streamline the recovery process. Redundancy also offers an alternative path for maintaining a systems functionality during a disturbance. Redundancy is expensive and counter to the typical optimization practices used in infrastructure management today, but it provides a means to ensure system functionality even if certain components are damaged or destroyed. Redundancy is most effective when redundant components are not physically located in the same area to ensure that redundant components are not disrupted by the same threat. By varying the location of redundant components, the level of diversity is also incorporated into the system (Yodo & Wang, 2016).

The next chapter will discuss the issues involved with incorporating resilience into communities and infrastructure management. The varying definitions and models discussed previously make resiliency management decision making difficult to quantify and replicate which leads to communities with varying levels of resilience depending on the definition chosen, the model used to quantify resilience and the strategy used to prioritize the limited funds available for resiliency. The issues with defining resilience and a resiliency framework faced by academia and federal agencies make resiliency management a difficult task at best for local government decision makers, infrastructure managers and other stakeholders.

Chapter 4. Issues Involved with Resilience

Communities and infrastructure remain woefully unprepared to cope with the effects of natural and manmade hazards even though infrastructure and community resilience has been a concern since the 1980s and a national level priority since PPD-21 and EO-13636 in 2013 (Presidential Policy Directive 21, 2013; Longstaff *et al.*, 2010; O'Rourke, 2007; Order, 2013). There are several issues involved with resilience and resiliency planning and budgeting that make incorporation of community resilience plans and strategies difficult, at best, to incorporate. The biggest issue in the current state of resilience strategy incorporation is the vagueness of the term resiliency caused by the numerous definitions, models, assessment frameworks, and prioritization of infrastructure strategies. There is no unified effort amongst government agencies to address these challenges and produce a single framework for community infrastructure managers and stakeholders. (Larkin *et al.*, 2015; Longstaff *et al.*, 2010). On top of this, the number of threats faced by communities and infrastructure systems and the increasing frequency of hazards over the last three decades make a comprehensive resilience strategy almost impossible to develop, as well as economically unfeasible (Guha-Sapir *et al.*, 2004; Longstaff *et al.*, 2010; O'Rourke, 2007). The complexity of modern infrastructure coupled with the age and degradation rate have compounded to make budgeting for resilience vs routine maintenance and repair difficult to manage for community, regional and national level infrastructure managers and decision makers (Ouyang *et al.*, 2012; Yodo & Wang, 2016).

This chapter will highlight some of the major issues with resiliency and resilience planning by discipline in order to frame issues that need to be resolved moving forward. This chapter will also break down the issues by the aspects of resilience according to the DHS sponsored Argonne National Laboratory definition of resilience which is "the ability of an entity-e.g., asset, organization, community, region- to anticipate, resist, absorb, respond to, adapt to and recover from a disturbance…" (Carlson *et al.*, 2012). Finally, this chapter will cover issues with funding resiliency in a budget constrained environment.

ISSUES WITH RESILIENCE BY DISCIPLINE

In order to cover the major issues faced by the concept of resilience, the issues will be broken down into issues faced by government agencies, academia and the industrial sector. The "government" is defined as the federal agencies and local infrastructure managers and local government that has to implement and execute policies and procedures in order to incorporate the idea of resilience. "Academia" is the institutions that develop the theory and resilience that are considered in the development of policies and procedures. Finally, the "industrial sector" is considered private businesses and public entities responsible for the economy and infrastructure management in the U.S.. Industry incorporates ideas from academia and is affected by regulations and policies enacted by the varying levels of government.

Government

The most pressing issue faced in the implementation of national level resilience objectives is the vagueness in the resiliency end state and goals of differing federal agencies. In other words, a clear set of community resilience objectives has not been defined for community and local government decision makers. Clearly defined and achievable objectives would encourage the incorporation of resilience into public policy and infrastructure management. State and local government decision makers and infrastructure managers have a difficult time operationalizing and defining quantifiable goals for resiliency (Meerow *et al.*, 2016). The lack of consistency and standardization caused by multiple frameworks and assessment strategies for resilience makes prioritization of community and infrastructure resiliency projects a subjective and qualitative task for most state and local governments. PPD-21 and EO-13636 guide the establishment of the varying federal agency definitions of resilience based on their individual roles or functions and does not dictate that the definition of resiliency in the directive is the only definition. A uniform and clear-cut end state with quantifiable goals is crucial in order to make operationalizing and measuring success of resilience initiatives feasible (Meerow *et al.*, 2016).

Communities and regions will inevitably be at differing levels of resiliency without a uniform framework for identifying vulnerabilities, assessing community resiliency, and prioritizing resiliency projects. If the variances in resilience preparedness are not addressed, then regional and national resilience will continue to be affected by those communities or systems within the infrastructure network that are not at a suitable level of resiliency. The complex interdependent nature of infrastructure systems causes any single failure within the network to have debilitating and cascading effects. For example, the 2003 Northeast Blackout, which affected approximately 50 million consumers, led to 11 deaths and caused an overall economic loss of $6.4 billion, was initially triggered by the failure of a few high-voltage transmission lines. In this case, the failure of transmission lines in the Cleveland-Akron area eventually spread across southeastern Canada and eight northeastern states within the United States (Longstaff *et al.*, 2010; Minkel, 2008).

While the definitions of resilience vary, academia and decision makers seem to agree that a lack of standardization, a central source of data, and tools leaves infrastructure facility owners, infrastructure managers and other decision makers without a clear guide to define and measure the resilience of their structures or systems (Carlson *et al.*, 2012;

Gilbert, 2010; Longstaff *et al.*, 2010). Effort is duplicated or repeated due to a lack of knowledge management across government agencies. There are frameworks that have been developed and tested in the U.S.'s nation building efforts to frame the problem of community resilience and develop resiliency strategies to address resilience. The DOD uses the PMESII-PT ASCOPE crosswalk framework, discussed in Chapter 3, which can easily be reconstructed to address individual community resilience efforts. By simply defining the "Military" aspect of PMESII-PT as National Guard, law enforcement and first responders, the crosswalk can be applied to U.S. communities (Walden, 2011). Assuming that this framework, or any framework is accepted, the issue would then become having all federal agencies buy into the concept and weigh in to address each individual agency's mission objectives.

Another issue is the constantly evolving political environment. Prioritizing spending on disaster preparation moves with political cycles, not necessity (Aldrich & Meyer, 2015; Healy & Malhotra, 2009). As political power changes hands from one party to the next, the objectives and political will to accomplish resiliency related goals waxes and wanes. While community resilience is a pressing issue, objectives of local governments change as new leadership changes out. The current subjective and qualitative methods for assessing and prioritizing resiliency is then not replicated the same way by each administration. A quantitative and repeatable method for resiliency planning and incorporation built into federal policies and regulations is sometimes the only way to ensure that an objective survives decision maker turnover. In some communities, like those along the gulf coast or those affected by earthquakes and wildfires, resiliency is a pressing topic that political leadership must constantly address. The number and types of threats also make resiliency an issue. Some communities have a very low perceived threat of different types of disasters, and therefore they only focus on one or two that have a higher likelihood of occurrence. For example, a midwestern town that produces corn or crops vital to the agricultural economy may only focus on the threats posed by tornadoes and draughts, yet a terrorist attack on that town could be devastating to the agriculture supply of the nation. This is evidenced by the romaine lettuce recall in 2018 caused by E. Coli. being found on lettuce produced in California (FDA, 2019). If there is a low or no perceived threat, or no perceived need, then political will to mobilize resources to protect against the threat is also low.

Another issue with the government is the incorporation of new academic theoretical ideas into practical approaches used to address resilience. There is often a disconnect between academia and real-world infrastructure managers and community decision makers. Sometimes this is due to the fact that academic research is often presented in a highly theoretical manner as opposed to being presented in a practical and actionable manner. The government often partners with few "think tanks" and not with all academic institutions (Larkin *et al.*, 2015). Regardless of how a good idea is presented there is a disconnect created by the process it takes to gain political traction for incorporation into regulations and application at the federal, state and local levels. Sometimes a groundbreaking idea does not make it to the appropriate agencies to be incorporated in a timely manner, sometimes the disconnect is due to the process of taking a theoretical idea and making it an actionable policy. This disconnect is not new, but it should be addressed in order to close the gap between resilience practitioners and stakeholders and academia.

Academia

The main issue in academia is the varying definitions applied to resiliency. In order to aid the government in applying a uniform resiliency policy, the five theoretical debates discussed in Chapter 2 should be resolved as applied to the governance of community and infrastructure resilience. Along this line the research conducted to accomplish a unified definition for governance of resilience, academic institutions should be mindful of the theoretical to practical application gap and tailor their products to ease the implementation of ideas into policy.

Another issue faced by academia is modeling and quantifying resilience. There are several models and methods for quantifying resilience depending on the field, but there is no one model for the governance and application of community and infrastructure resilience. The closest and most widely accepted model is the resiliency triangle and four R metrics of resiliency introduced by Bruneau *et al.* (2003). The issue with the development of most quantifiable models for resilience is the lack of data or the lack of access to data for the various metrics identified in research. Resiliency data after storms or other hazards is sometimes considered classified or close hold by the government. With the number of international researchers in academia the ability to release sensitive data is sometimes an issue. There are several methods to address this issue and decision makers will have to develop a means of addressing the access to data for future resilience related research. Data collection during a natural or manmade hazard is another issue because it is hard to forecast when data can be collected. Incorporating knowledge management into disaster situations is often done retroactively and therefore vital information is lost. One way to address this issue is to incorporate knowledge management into resiliency strategies.

Another issue identified is the number of "all encompassing" literature reviews and tools available that differ depending on the time they were created and the direction or discipline that the author was taking when amalgamating the information. The wide array of tools and literature makes applying academic ideas difficult for those attempting to develop actionable policies and regulations. This research is an attempt to develop a single source of the most pertinent information for the development and application of resiliency strategies in policy making and governance related to resilience improvement.

Industry

Industry is typically concerned with economic resilience, organizational resilience, engineered resilience and industrial systems and process resilience. Industry incorporates academia developed theoretical ideas into their systems and processes that are also regulated by policies and regulations of various levels of government. The disconnect between academia and the government policies can lead to friction when applying theoretical approaches. Sometimes an idea may be prevented by government regulations, again highlighting the need to close the gap between academia and governmental agencies.

PREVENTION, MITIGATION, RESPONSE AND RECOVERY

Since the DHS is the only agency with resilience as a direct part of its mission statement this thesis focuses on the Argonne National Laboratory's definition of resilience. The definition mentioned previously has six abilities of an entity with regards to changes caused by a disturbance (anticipate, resist, absorb, respond, adapt to and recover from a disturbance) that can be categorized into four phases of resilience. Prevention is concerned with the ability to anticipate change, mitigation considers the abilities to resist and absorb change, recovery is concerned with the abilities to respond and adapt to change and recovery is concerned with the ability to recover from changes associated with a disturbance. Issues with each phase will be discussed in order to identify where technology can be applied to address ability gaps or vulnerabilities (Carlson *et al.*, 2012).

Prevention

There are five major issues that affect prevention or the ability of a community to define and anticipate the hazards that it faces (Carlson *et al.*, 2012). Choosing the proper framework for framing the issue of resilience and assessing itself can be a daunting task because there are numerous methodologies depending on the government agency addressing resilience and the academic model chosen to define the environment. Also determining the proper prioritization of resiliency improvement projects depends on the local community decision makers qualitative assessment strategy. The prioritization of projects is therefore subject to change between political power brokers and may lead to wasted time and funds. Different prioritization strategies can lead to inconsistent resilience preparedness within a region. The number of threats faced by a community are hard to define and address due to the complexities of modern communities and infrastructure (Larkin *et al.*, 2015). Finally, funding resiliency improvement projects in a community is an issue due to the limited amount of resources available. Prioritization of resiliency improvement projects is therefore critical and dependent on the policies of the decision makers and infrastructure managers.

Mitigation

Issues with mitigation are compounded by the issues with preparedness. Mitigation is the activities taken prior to an event to reduce the severity of a hazard (Carlson *et al.*, 2012). Mitigation activities are typically constrained by time and are based on the action plans determined in the preparation phase. Local governments typically have pre-negotiated contracts with private entities to execute the action plan. The problem with this process is that not all communities have the contracts they need in place which leads to inconsistencies in mitigation activities throughout a region. Mitigation activities are also determined by the prioritization of resiliency activities laid out in the preparation phase. The ability to shore up protective measures prior to an event are based on both material resources, personnel available and the amount of time to prepare for an event. Planning, once again is key to mitigation activity prioritization. The mitigation plan is also highly dependent on the resiliency strategy chosen. A community can rely on either redundancy, resourcefulness, rapidity, or any combination thereof to design their overall strategy to mitigate hazard consequences. Once again, variance is introduced in the level of mitigation depending on the strategy chosen.

Response

Response is the immediate activities, tasks, or programs that have been developed to manage the adverse effects of an event or hazard (Carlson *et al.*, 2012). Issues with response are the same as those found in the planning and mitigation phase. The ability to respond and adapt to an event is dependent on the plan that is chosen and the preparations made prior to the event. Response is the phase that is most contingent on the capabilities of the decision makers and requires immediate and continuous situational awareness, assessment and sound decision making. The human aspect is most involved in the response phase and will vary between emergency response coordinators and those in charge of a community.

Recovery

Recovery includes the programs designed to effectively and efficiently return conditions to a level that is acceptable to the entity (Carlson *et al.*, 2012). The issues with recovery are contingent upon the definition of resilience chosen. Acceptable conditions may be the same as prior to a disturbance or event or it can be a condition that is improved from the original conditions. Strategies for recovery and prioritization for recovery projects are also a factor in recovery, where the focus is on how funds and resources are managed and prioritized in order to recover systems damaged by a disturbance, hazard or event. The timeline for recovery efforts can be either in days, weeks, months, or even years, depending on the priority of the system being recovered as defined by decision makers, infrastructure managers or private stakeholders.

FUNDING

According to the ASCE, the infrastructure in the U.S. is in a dismal state and requires an additional $110 Billion in investment by 2025 in order to get to desirable conditions (Denecke, 2018; Türk, 2013).The deteriorating infrastructure competes for the same constrained budget as resilience improvement projects, many of which are centered around the infrastructure mentioned in the ASCE report. Coastal resilience is a hot topic in the U.S. due to the rising number of natural disasters like hurricanes, that affect coastal regions (Guha-Sapir *et al.*, 2004). Another disaster type that is in the forefront of resiliency development is the wildfire threat faced by the western portion of the U.S. Like infrastructure, short term goals outweigh long-term resiliency objectives and therefore, resiliency enhancement is losing most, if not all, of its funding to short term prevention. In the case of wildfires, fire suppression and response costs used most of the funds available and left little if any for long term resiliency and prevention (Stephens *et al.*, 2016).

Public-Private Partnership

There are some methods to ease the economic burden on the government like public-private partnerships (PPP) or governments contracting private businesses to construct infrastructure. The private business is then allowed to run and collect revenue from those projects for a given number of years alleviating the government's economic burden of resiliency improvements to physical infrastructure. Innovative investment strategies, if incorporated properly could be a major benefit to resiliency enhancement in the future. However, there are issues involved. PPP projects are sometimes conducted over several years and involve risk for the investors. If the agreed upon regulations, like higher speed limits on roadways to ensure traffic use, are changed by policy makers then the investors could lose a significant amount of revenue. Shifts in political policy regarding the management of infrastructure, in some instances, make private investments risky for companies involved in providing services for compensation that are normally viewed as a right by the public.

Economic Disincentives

The economic disincentive to some infrastructure systems, like smart water, is the idea that some services must be delivered at the lowest cost. Utility providers know that providing a resilient infrastructure system will benefit society in the future, but there is no economic benefit to a private business in spending money on resilient infrastructure. If resiliency is not a design specification, which it typically is not, then companies will put in the most efficient infrastructure. Efficiency, most of the time, means using the cheapest material and reducing redundancy and reliability to a level that meets the minimum acceptable requirements of a contract. Minimum redundancy and reliability reduces diversity and resiliency in the infrastructure system as a whole. Tax breaks and other incentives may help with this, but they cannot completely defray the construction costs. Raising the cost of some infrastructure services to offset the cost of designing and building for resiliency is politically risky. Therefore, most communities will not place resiliency as a design specification unless there is regulation or a compelling reason for the community to do so. For instance, a water distribution network, unlike the power distribution network, does not produce the same market for utility companies as power does. Differences in the profit margin for the management of infrastructure make PPPs, as well as other alternative means of funding resiliency, viable in some infrastructure systems and not viable in others.

Chapter 5. Technologies for Resilience Improvement

This chapter will cover some of the technologies available that can be applied to community and infrastructure systems in order to improve resilience. The list in this chapter is not an exhaustive one. It is simply meant to point out some of the emergent technologies that can be applied to solve current issues in resilience planning, infrastructure management, furthering the development of resilient communities in the future. Determining how these technologies can be used to solve the issues identified will be discussed once some of the applicable technologies are identified and defined.

APPLICABLE TECHNOLOGIES

The applicable technologies discussed are broken down into three sections: technologies that are available to be applied to infrastructure and community systems now, technologies that are currently under development or need to be developed for future application and technologies that are needed but are not in development, specifically for infrastructure and community resilience. These three sections provide a way to divide technologies into levels of development and/or research to provide infrastructure managers and community decision makers with an idea of the state of these technologies and if they are worth looking into for investment now, or in the future. The technologies outlined are not a complete list, but can be used to show how some of them can be used throughout the phases of an event to improve the resilient response to disturbances while containing the negative effects of cascading failures.

Technologies Available

Information and communications technologies (ICTs) are technologies that apply to the sharing of data through telecommunications. Telecommunications can be in several different platforms including telephone lines, fiber optic lines, wireless networks, cell phone networks, computers and the internet. The use of ICTs is critical for collecting and communicating data for analysis and decision making. As infrastructure and community systems become more interconnected using smart sensor networks and other technologies described later, several different types or levels of ICTs will exist as communication technologies evolve. In order to solve the communication issue between different generations of technology (IE 2G, 3G, and fiber optic) the Next Generation Mobile Networks Alliance has begun work in developing self-organizing and self-healing networks to minimize human intervention in planning, deployment, optimization and maintenance of ICT networks.

Future networks will be able to communicate between nodes consisting of different technologies. The future network would use each node as a receiver and transmitter to communicate data from an infrastructure system to the data center. If one node goes down, then other nodes would be able to identify the issue and bypass the node until it can be repaired (Ramiro & Hamied, 2012).

ICT usage can also define how decision makers and infrastructure managers not only communicate and control their systems, but also how they connect and pass information to their constituents or customers. By using different social media and smartphone applications future infrastructure and community leaders can either be effective in the use of ICT or they can be ineffective and create conditions in which their individual community is less resilient. Using ICT to disseminate information and organize the community can be done effectively if messages are crafted properly. ICT can be used to improve not only management of infrastructure but also its use in times of crisis. For instance, the amount of people on the road during an evacuation could be somewhat controlled by sequencing the dissemination of an evacuation order. Road congestion caused by an evacuation order may be somewhat mitigated by phasing the dissemination of an evacuation message from those communities that are in most danger to those that are in least danger. While the idea of "phasing" an evacuation order may cause equity concerns it is an idea that may aid in decongesting evacuations. Another means to control an evacuation is sending different groups in different directions by varying the evacuation information (Chewning *et al.*, 2013). ICT is often tied to the concept of the internet of things or IOT (Holler *et al.*, 2014).

Having several sensors communicating data about an infrastructure network creates the ability to measure and understand the infrastructure system, how it is interconnected with other infrastructure systems and the environment in which the network lies. This sensor network creates an internet of things or IOT. The idea of IOT is to blend sensor data with actuators controlling the infrastructure network to create a common operating picture that can interact with decision makers or infrastructure managers in order to optimize operations. This technology is available and can be applied to infrastructure and community systems through the application of sensors, meters and other forms of data collection devices in use today (Gubbi *et al.*, 2013).

The next important technology available for application is global positioning system (GPS) technology. GPS technology uses satellites to identify the location of different nodes and sections of infrastructure and community systems. GPS technology would help with not only mapping the infrastructure in existence, but also locating problems and modeling the network for optimization. GPS technology aids in IOT and ICT technologies as well as data analysis. The amount of data that would be transferred by infrastructure systems alone needs to be collected, organized and analyzed for decisions.

GPS combined with wireless technology create the ability to communicate not only data about the system but also the location of the issue. Wireless technology relies on towers to collect and transmit signals containing data from one area to another. This information paired with information about other interconnected systems like the community physical and social structures can be combined and controlled using big data and Supervisory Control and Data Acquisition (SCADA) technology discussed below.

Big data is the technology and processes involved with collecting massive amounts of data, organizing it, and then analyzing it to inform decisions with regards to the operation and efficiency of infrastructure and community systems. Big data will become increasingly important as nodes begin to report large amounts of information that could overwhelm decision makers as they try to manage community resilience. Big data incorporates mobile computing, GPS, modeling software and wireless technology to create a picture of what is going on in the network for decision making. Mobile computing has been around for a while and makes interacting with the network easier. Laptops and smartphones give everyone the platform by which to interact with infrastructure, community and emergency response systems.

Using mobile computing as a platform and big data feeding the information for decisions, it is necessary to create a medium for which to control the network. Modeling software like Supervisory Control and Data Acquisition (SCADA) technology takes all of the information and places it on a virtual network map. SCADA allows decision makers and infrastructure managers to interact with and make decisions to maintain, repair or optimize the network. SCADA networks are self-healing and able to control the functionality of the system through interacting with Programmable Logic Controllers (PLCs). PLCs located within key infrastructure systems like pipeline networks, the electrical grid and transportation infrastructure allow decision makers, infrastructure managers and stakeholders the ability to control the functionality of infrastructure systems. SCADA allows the ability to optimize operations and visualize what is going on within the infrastructure network (McCrady, 2013).

Smart meters and sensors are able to transmit data pertaining to the amount, pressure, voltage and flow rate of key resources, such as, energy and/or water passing by the meter or sensor wirelessly. This technology is available and in use in some water and power networks across the U.S. Smart meters cut down on the time it takes to collect data about a network and identify issues in the system as well as inefficient use or transportation of power and water. For example, if water, power, or traffic passes one point in the system with a certain amount of pressure, voltage and/or flow and then passes another smart meter with less pressure, voltage or flow, the decline indicates a problem with the infrastructure network between the smart meters. Combining smart meters with GPS and modeling software allows the infrastructure managers and stakeholders the ability to pinpoint issues and address them, saving time, money and resources previously used to hunt down the issue within the infrastructure system in question.

Another technology that can be applied to infrastructure networks, improving the dependability of infrastructure on the power grid, is solar and hydroelectric technology. Advancements in turbine power production has created mini-turbines that can be applied to the infrastructure network to provide power for various operations. Advancements in solar technology are making solar panels more affordable to homeowners allowing them to place panels on their homes, or for infrastructure managers to build into photovoltaic (solar power producing asphalt) roadways. Mini-turbines combined with advancements in less expensive solar power would offset the reliability of infrastructure on the power grid, increase the diversity within infrastructure and make a city more resilient through redundant power generation sources.

Photovoltaic roadways have the potential to decrease the reliability of society on fossil fuels, making electronic vehicles more feasible as the roadways could have the capability of charging the vehicle while driving on the road surface (Mehta *et al.*, 2016; Patent, 1986). Another technology that has promise to reduce reliance on power grids is power storage technology. Developments in technology to store power for extended periods of time is a recent development that has the potential to provide buildings and key infrastructure nodes (hospitals, stop lights, etc.) with the ability to have backup power stored. Backup power would provide decision makers and infrastructure managers with more time to repair, and shift manpower or resources as necessary to counter any adverse threats or interruptions without major loss in infrastructure functionality.

Advancements in water storage systems would also improve the resiliency of a community or city water supply. By increasing the amount of water stored, as well as the ability to treat water being held in storage systems throughout a water network, would improve the resilience of a water network and mitigate issues caused by drought or physical attack on the water network. Ultraviolet treatment and other water purification processes can now be completed at a much smaller and affordable scale. Applying new storage technology could improve both water network efficiency and water quality for the end user. Additionally, advancements in water storage could allow households and other surfaces that produce high runoff some capability to store water either for treatment and use or to provide the community with additional reservoir capacity. New storage capacity would improve community resilience to floods and droughts by providing alternative and diverse stormwater storage and water sources. The additional storage capability, under the control of infrastructure managers, could relieve the pressure on levees, stormwater systems and reservoirs during flood and flash flood crises. During droughts water treatment facilities could draw on the additional storage to fill water shortages. Similar advancements in the capability to store power in batteries could also have positive impacts on community resilience by reducing reliance on the power grid.

Promising Technologies Under Development

Promising technologies under development are technologies being applied to other areas that should be developed for community resilience. Technologies under development apply to both virtual and physical components of infrastructure and community resilience and require both research and testing before they are viable options. Infrastructure systems of the future will produce a large amount of data from an increase in sensors used for monitoring and control. The data produced will need to be protected from cyber threats to both individual citizens and the infrastructure system as a whole.

Block chain is the collection and storage of data over several different servers and platforms to increase the security of data and make it difficult to access by those not authorized. Block chain technology is in development but has not been applied to infrastructure data. The reason for not applying it to infrastructure is mainly due to the limited amount of data produced by current infrastructure systems. As discussed previously, infrastructure systems are becoming more interconnected with the use of smart technologies that require large amounts of data and block chain could be applied to ensure cyber security (Mylrea & Gourisetti, 2017).

Sensor technology is the means by which information about a network or environment can be accessed. Sensors are being developed with more functionality at a smaller size. The idea that many small sensors can be used in conjunction with each other to collect data is called sensor swarm. Sensor swarms have many implications for future infrastructure resilience. Microscopic sensors in the water distribution network, for example, that can easily be filtered out can provide massive amounts of information about water as it passes through a water distribution network in real time. While sensor swarm technology is in development, it still has yet to be applied to infrastructure and community systems to improve resilience (Xu, 2002).

Drone technology is being developed for commercial and military applications throughout the U.S. Drones are becoming smaller and have a greater capacity to interact with their surroundings. Submersible drones as well as flying drones could be used in the future to ensure security of and conduct maintenance on infrastructure networks. Drones could also be controlled by Artificial Intelligence (AI) developed for the purpose of ensuring the efficiency as well as resiliency of infrastructure and community systems. There is also development in using drones as communication nodes to replace damaged or overloaded cell towers. A self-healing swarm of drones capable of receiving, transmitting, or retransmitting communications signals could ensure continuity of communication services for the population along with emergency responders (Hayajneh *et al.*, 2016; Naqvi *et al.*, 2018).

Water harvesting technology is in development in areas with limited or fluctuating access to water. Cities and communities currently have access to about thirty percent of the hydrological cycle or fresh water available. Distillation and desalinization technology as well as additional means of harvesting water from the environment can be used to improve the percentage of water available to communities. Examples of water harvesting technology is distilling fog into water and using sunlight and soil moisture content to access water previously not available for consumption. While this type of technology is available it is not efficient enough at this time to produce water on a scale that provides an economically viable redundant water source (Postel, 2000).

Interactive applications are used by people every day to interact with their environment. These applications improve everyday life and actually make use of electricity and other utilities more efficient. Interactive applications need to be developed for the smart infrastructure systems of the future. For example, these applications could be used in conjunction with smart meters and filtration systems in order to provide the end user with the ability to control the amount and the quality of the resources they consume or use. If, for instance, a homeowner is going on vacation they would be able to turn down the amount of water and electricity provided to their home without disrupting service. This would lower the users bill and provide the community infrastructure systems with more resources to be redistributed elsewhere. Interactive applications applied to the resource delivering infrastructure systems would provide greater efficiency and possibly redundancy for the community and infrastructure systems as a whole.

Technologies Needed but not Available

Technologies needed but not available are technologies that are needed to enable or improve community and infrastructure resilience in the future. These technologies are used to apply current technologies to community and infrastructure resilience or to create conditions that would allow technologies in development to be applied to communities for infrastructure resilience. Future advancements may make these technologies available and more applicable to the physical and social aspects of community infrastructure system resiliency.

Optimization algorithms have been in development for decades and can be easily applied to simple systems. They are used to model and identify where a network or process is inefficient and what can be done to improve or optimize the process. These algorithms need to be improved and applied to more complex systems such as road networks, power distribution networks, or urban water distribution networks. Algorithms could be designed to optimize resilience under different threats and combined to create an all-threat simulation and/or system that is able to respond to different threats quickly and efficiently while minimizing cascading effects of single failures. These algorithms would enable quantum computing and artificial intelligence to be applied to infrastructure systems of the future.

Quantum computation and quantum information is built on the principles of quantum mechanics by using information on natural behavior to run algorithms designed to process information in a more holistic manner. Quantum computation may lead to revolutionary breakthroughs in materials, optimization of complex systems, artificial intelligence, and resilient infrastructure systems and communities. Quantum technology is in development but would need to be designed and applied to resiliency of infrastructure and communities in the future to enable the use of artificial intelligence (Ouyang & Fang, 2017).

Artificial neural networks (ANN) and artificial intelligence (AI) are technologies that are used to replace human interaction with computers. Artificial neural networks use nodes, much like the smart meters and PCLs described above, to create a network that interacts much like a human brain. ANN combined with the algorithms created by quantum computing would allow a computer to identify issues, make decisions, and affect the network using AI. This technology is applied to other sectors but could easily be applied to infrastructure and community resilience. By collecting data and analyzing how that data drives decisions, then feeding this information into a computer a database of past experience can be built for a computer to make future decisions. Knowledge management at this level is not available today. Knowledge and experience is lost as decision makers and infrastructure managers change out, retire, or are replaced. A computer database would create AI that can understand the environment of a city or community and make decisions based on experience in order to optimize infrastructure system operations and replace human decision makers and managers with computer technology (Naoum *et al.*, 2013).

Smart materials refer to physical materials that can be applied to physical infrastructure systems to improve sustainability and operations. Smart materials in the future could theoretically monitor all aspects of the resources or traffic passing through or utilizing an infrastructure network. For instance, if there was a leak in a pipe the pipe would recognize the issue and be able to adjust its properties to close the leak and report the issue. Another example would be if a roadway has a traffic jam during an evacuation, signs could change that lead further traffic elsewhere to avoid the congestion. Smart materials like sensor technology and pipe lining or covering that can self-monitor and adjust to ensure optimal performance of that section of pipe enable these two examples. Another example of a smart material in development is pavement that can self-identify as in need of repair, or self-healing. Smart pavements could turn a different color as conditions in the pavement or pavement structure changed in an unfavorable way. This would allow infrastructure managers or AI to easily identify issues and dispatch repair resources immediately, or as the priority arose (Cao, Cudney, & Waser, 1999).

Another technology or system that could be developed to enhance infrastructure and community resilience would be inter-city interaction mediums. This technology would be a way that cities or communities could share information about their community infrastructure system operations with other cities and provide lessons learned or procedures that might benefit other cities and networks. Shared information would allow other cities to benefit from the experience of other cities to make all threat resilience a reality. Improving pre-disaster planning and preparation would allow entire regions and the entire nation to be more resilient. These interaction mediums could be everywhere from a database to a human convention designed to share ways to optimize resource allocation or operation of infrastructure systems. Perhaps future resiliency projects could make it possible for neighboring cities to share resources in times of a disturbance or provide aid in a time of crisis.

These technologies are not the only technologies that could improve community and infrastructure resilience in the future, but they are a good representation of the technologies needed to improve community resilience and ease the burden on decision makers and infrastructure managers. As future technologies and ideas are developed, this list of technologies should be amended to accommodate future advancement of community and infrastructure system resilience policies, operations or infrastructure network resilience.

APPLICATION OF TECHNOLOGIES TO RESOLVE ISSUES WITH RESILIENCE BY DISCIPLINE

In order to demonstrate how the technologies introduced in this chapter apply to the issues presented in Chapter 4, this chapter will break down how technologies can be applied by discipline. Resilience as a theory will still have multiple disciplines and focus areas, but the application to community and infrastructure systems resilience can be simplified. A common resiliency goal depends on developing unified effort to determine a framework for developing resiliency strategy, a method for prioritizing resiliency projects and assessing resilience in communities.

Government

Developing a unified framework for resilience strategy across all levels of government based on a single definition of community and infrastructure systems resilience is essential to ease the burden on community decision makers and infrastructure managers. The multitude of frameworks available must be filtered down to a broad and scalable, but quantifiable means of assessing the current community physical and social environment while designing an actionable strategy to prioritize resilience projects at all levels of the budgeting process. The system must include methods for assessing progress as well. Big data, blockchain, optimization algorithms and SCADA can be used to create a national, regional, state and local database that shares information both up and down the chain to ensure knowledge management and interagency collaboration. As infrastructure systems continue to develop and incorporate sensors and smart technologies, data should be collected and shared to glean lessons learned for other communities to benefit from. New technologies make infrastructure more interconnected while providing new sensor networks and data sources that can be analyzed and shared across different types of infrastructure by decision makers, infrastructure managers and researchers alike.

It is important to ensure that frameworks for resiliency strategy and project prioritization should be quantifiable and easy to justify and replicate so that the chosen methods are resilient to political turnover and shifting policies and priorities. As knowledge management improves from the use of a single database an all-threat design will become easier. Also, ANN and AI will benefit from lessons learned by communities across the nation that face different threats at different levels of importance by region. Blockchain can ensure that the efforts and knowledge gained by a single database is protected because the data can be stored in a variety of physical locations which would provide diversity to the database infrastructure.

Academia

Academia should be encouraged with incentives to think about the development of a single resiliency database and methodology for community and infrastructure system resilience. Academic researchers should be able to access data critical to modeling and designing optimization algorithms to aid in knowledge management and resilience project prioritization. No one academic institution or research entity should be responsible for developing resilience strategies. Academic institutions, while benefiting from federal funding, would be able to multiply the manpower of the federal resilience initiatives and prove to be a resource multiplier in the development of resilience frameworks and methodologies. Academia would also benefit from lessons learned that have been provided by resilience decision makers, practitioners, managers and other stakeholders. Access to a single knowledge management source could provide academic institutions with the information necessary to develop actionable recommendations and frameworks in the advancement of community and infrastructure resilience.

Industry

Industry can also be used to feed the database organizational resilience lessons learned. Each individual business entity can provide lessons learned from successes and failures in varying approaches to the use of ICTs and system process adjustments in the face of disturbances. Industrial and business entities would benefit from access to knowledge management in the prevention, mitigation, response and recovery phases and provide actionable feedback to government agencies for the development of resilience policies.

Using sensors throughout industrial processing allows a company to collect and analyze more data to optimize their production processes. The sensors and controls within an industrial plant can then be controlled using SCADA programs. The data collected from these processes can then be analyzed and capitalized on using optimization algorithms. ANN and AI could use that data to gain knowledge and be able to run the industrial process with little to no human intervention. All of the data produced can then be protected with block chain technology. All of these technologies have the capability of making a process more resilient if resilience is a design parameter. The use of computers to not only identify and optimize not only an industrial process, but also optimize the resilience of that process would ease the burden on industrial leaders to decide where and how to spend limited resources. Advanced technologies, if applied properly would significantly improve organizational and industrial process resilience. The only limitation is an organizations willingness to adapt and apply new technologies.

Chapter 6. Identification of Research Needs

Chapter 6 will discuss the areas that still require further research in order to facilitate the implementation of resilience policy improvements to enhance resilience throughout the U.S. by improving resilience, resilience public policy and the social and economic impacts of resilience. In order for community and infrastructure resilience to become more implementable certain areas of future research are necessary. The research required involves physical, social and virtual components of resilience, as well as the second and third order effects of implementing resiliency policy. Identifying research that needs to be completed for resilience to be implemented, is important in identifying gaps in the government's current policies and procedures.

IMPLEMENTATION OF RESILIENCE

Replacing, maintaining and upgrading the current physical infrastructure systems has several components that need to be researched. One is the most effective means of sourcing funds to conduct resiliency improvement projects is additions to the current funds allocated to routine maintenance and operating costs. In the current fiscally constrained conditions faced by government at all levels, it does not seem likely that the money to improve community resilience will be available. Each community should look into the best sourcing solutions to acquire the funds necessary for resiliency projects. Options for sourcing solutions include private-public partnership, raising the cost of services provided by infrastructure, or prioritizing funds remaining after routine costs for the purposes of resiliency improvement. Research is required in the area of options funding resiliency in order to move from current pressing issues and move towards long-term resilience goals.

Another topic that needs to be researched concerning the physical system is how to replace the current infrastructure with more advanced resiliency focused features. Replacing the system in a piecemeal fashion as components deteriorate will not provide the scale necessary to achieve resilience goals. If resiliency features are only incorporated in newer parts of cities or one part, as opposed to another, then access to the benefits of resilience will be unequitable and may cause issues in the community.

Research into how to close the gap between academia and government implementation of resiliency improvement ideas, models and theories is also required. The data required to conduct in-depth modeling and research surrounding resilience implementation is difficult at best to access and is located in several different locations that are not easily accessible. Researching how to pool this data into one centralized databank focused on resiliency improvement is recommended to make this process easier. Also, research into allowing access to resiliency related data deemed classified or close hold by the government is required to facilitate the implementation of a centralized resiliency database for the improvement of national resilience efforts.

TECHNOLOGIES TO IMPROVE RESILIENCE

The next topics that need to be researched are how to apply technologies to infrastructure systems, the effects of technology on infrastructure decision making and management, how fast to implement new technology and measures of effectiveness on resilience improvement projects. A community needs to know the positive and negative effects of applying technologies as well as how to prepare for new technologies that can potentially change the policies in place to manage infrastructure. If a community needs to phase in resilience technologies, then a strategy must be developed to provide guidelines for the pace and phasing of technology related resiliency improvement projects and for measuring the effectiveness of the new technology related resiliency projects. Technologies and ideas such as ANN, AI, optimization techniques and quantum computing could have a major impact on decision making and infrastructure management. A community would need to know how to identify the effects of resiliency improvement projects and when the community can expect to see those results.

Another research topic is to identify and optimize the way that a community prioritizes technologies and projects for resilience in order to make resilient communities and infrastructure more feasible. Research into prioritizing resilience technology improvements for the efficient use of limited resources and quantifying criteria for resilience related decisions is needed. Communities will differ but research should consider scalability and flexibility of frameworks for resiliency implementation to enable actionable options at the local level.

RESILIENCE PUBLIC POLICY

In order for resiliency improvement policies to be actionable and effective, the government, at all levels, needs to research the options for the best resiliency assessment frameworks, resiliency improvement strategy and resiliency project prioritization methods. The federal government needs to research and apply standardized goals and objectives for resiliency improvements, funding and incentivizing resilience as well as laws and regulations for improving resilience in the nation. One solution could be to create or appoint a federal agency for the single entity responsible for resilience related issues.

State and local governments need to research ways to prioritize projects, incentivize resiliency and ways to manage resilient communities and resiliency related improvement projects. All levels of government need to identify which means of incentivizing resilience is the most efficient and feasible way to encourage resiliency growth (e.g., tax breaks and/or a reward system for resiliency objectives achieved). The government should also research the best way to fund resiliency from outside the government budget (e.g., PPP vs private incentives for the industrial sector vs resiliency built into public project related construction codes or specifications).

SOCIAL AND ECONOMIC IMPACTS OF RESILIENCE

The second and third order effects of resiliency improvement policies, regulations, and procedures need to be considered as well. Examples of questions that should be answered include: Is regulating resiliency into building codes or specifications for infrastructure economically and legally feasible? What will be the positive and negative impacts of resilient communities? The positive and negative impacts of resiliency need to be identified so that the federal government can be prepared for the next step in managing resilience improvements. Inevitably some regions or states will be more willing and have more ability to implement resilience than others; and resources may need to be reallocated to ensure the equity of resiliency improvement throughout the country. The government needs to ensure that all regions, or sectors, are receiving the funds they require in order to ensure the resiliency of the entire nation. The government should research the benefits of resiliency strategies (e.g., improving critical infrastructure resilience first vs focusing on one or two key regions overall resiliency first vs small resilience improvements across the entire U.S.) and determine which one is most cost effective and efficient.

By answering the research topics outlined previously, the government at all levels will be better prepared to assist and provide the references and tools required by decision makers, infrastructure managers and stakeholders to act on resiliency policies. Phasing in of technologies and smart infrastructure systems into communities will aid in the accomplishment of resiliency related objectives; and the research outlined in this area will aid in understanding the effects of technological improvements to communities and infrastructure. Finally, the research related to the second and third order effects of resilience will aid in understanding which overall strategy should be chosen and the expected outcomes to determine measures of effectiveness throughout the phases of resiliency implementation.

Chapter 7. Conclusions

Resiliency is a topic of significant interest to academia and the government due to the increasing number and types of natural and manmade threats faced by communities and their infrastructure. The definition of resilience varies by discipline and overall objectives making the term almost meaningless without context. The number of threats combined with the complex and interdependent nature of modern infrastructure and community systems makes resiliency management and decision making a complex and difficult task. This thesis reviewed and compiled resiliency definitions and models, framed issues with community resilience management and policy making, introduced possibilities for applying technologies to solve resiliency issues and introduced actionable recommendations to improve community and infrastructure resilience management.

FRAMING THE PROBLEM OF RESILIENCE

The first issue with resilience that needs to be addressed is the lack of a unified definition of resilience for community and infrastructure on which all levels of government can base resiliency strategy and improved policy development. This issue leads to parallel lines of effort that often cause duplication of work and inefficient use of resources applied to resiliency improvement. There is also a lack of a single resiliency database and unified resiliency research center. Data is difficult to gather when attempting to research and develop strategies for community and infrastructure resilience. There are no unified efforts within the government and/or academia to address resiliency improvement strategies, which leads to several different methods to assess the current state of community and infrastructure resilience and different measures of resiliency improvement effectiveness.

The complex and interdependent nature of modern infrastructure and community systems along with the number of and variance in threats faced by communities makes a unified resiliency improvement strategy difficult to establish. Federal government agencies have attempted to address resiliency from the perspective of each individual agency mission which creates several methods and models for community decision makers and infrastructure stakeholders to choose from. No single unified, scalable, flexible and adaptable resiliency strategy and assessment methodology has been established to ease the burden of community resilience improvement decision making on community stakeholders. Without a unified framework, resiliency levels vary significantly across the nation and across the spectrum of governance. Federal agency's resiliency efforts are siloed and therefore inefficient in improving national resilience.

Another issue is that the aging infrastructure within the U.S. which requires $2 Trillion in additional investments in order to maintain the current level of service expected of our infrastructure (according to the ASCE's (2017) Infrastructure Report Card). The limited resources available to fund resiliency improvement projects must compete with immediate priorities leading to communities focusing on short-term goals, as opposed to longer term investments in community and infrastructure resilience. On top of the resource allocation issue there is no unified quantifiable means for prioritizing funding for resiliency improvement projects. The current subjective and qualitative methods are subject to change based on decision makers' changing roles or shifts in political will. If one local political party switches out, the prioritization of resource allocation is subject to change without a quantifiable and repeatable method for justifying the application of resources to resiliency improvement projects.

COMPARING MODELS AND FRAMEWORKS OF RESILIENCE

There are several models and frameworks for approaching community and infrastructure resilience available from both academia and the federal government. These models and frameworks vary based on discipline and goals in academia as well as being based on differing missions and objectives of federal agencies. Three basic differences in the models or frameworks can be boiled down to the approach taken to address infrastructure and community systems. The three basic approaches are: *risk assessment models*, *vulnerability assessment models* and *resilience improvement models*. Risk assessment models focus on the risks associated with failures coupled with the risk that a particular entity faces from varying threats. Vulnerability assessments are similar to risk assessments where the focus is on how vulnerable a system is to different threats based on the vulnerability of each component or entity within the system and how a failure will affect the whole system. Vulnerability and risk assessment models rely on data from past events and tend to be more reactive and not adaptive to new or unexpected hazards or threats. Resiliency planning takes vulnerability and risk assessments into account while addressing an entities ability to anticipate, resist, absorb, respond to, adapt to, and recover from a disturbance. Resiliency planning and improvement is the most encompassing method for improving the ability of infrastructure or a community to react to and recover from a disturbance in an adaptive and proactive manner.

FUTURE DEVELOPMENT

The future development of infrastructure and community resilience require funding sources and strategies in order to apply limited resources that address the short-term maintenance and operations costs while providing the ability to fund long-term resiliency objectives. Innovative or new PPP funding sources provide examples to find new means to access the resources required to accomplish both routine operations and maintenance costs, as well as resiliency improvement projects. Another means to accomplish overall resiliency improvement is to incentivize private industry resilience to require resiliency to be designed into the specifications of future infrastructure and community systems.

As communities incorporate technologies into their infrastructure and social systems, decision makers and infrastructure managers will need to consider how the new technology affects overall resilience. New technologies applied to resiliency improvement should be incentivized or required through design specifications. New sensor technology, along with the supporting IOT and ICT technology, require the ability to handle and process large amounts of information. New technologies will provide decision makers and infrastructure managers with the ability to better understand their systems and quantify the requirements to improve the overall resilience of the community and/or infrastructure. Technologies should also be applied to empower community stakeholders with control and execute the decisions they make by allowing changes to be implemented through SCADA, or similar control technologies.

RECOMMENDATIONS

The first and most important recommendation to improve the overall resiliency, resiliency strategy and resiliency assessment efforts is to establish a single definition and a unified effort to accomplish the varying resiliency objectives of communities and infrastructure. A single database and research effort would ease tensions, the effects of duplicated efforts and provide community resilience stakeholders with a standardized streamlining of resiliency related efforts.

Strategic planning frameworks exist within the government. These frameworks should be applied to resiliency in order to frame the problem and establish mutually supporting lines of effort to accomplish resiliency improvement goals and objectives. Through quantifying unified resiliency goals, the challenge of addressing resiliency improvement at the community level can be eased. Funds should be prioritized for resiliency improvement through identifying the quantitative objectives and incentivizing the accomplishment of those goals. Incentives can be applied to PPP funding sources or to individual industry and infrastructure sectors to encourage resiliency improvements that effect the community, regional or national resiliency. Another method is to require resiliency to be designed into project specifications. It should be recognized that there are several methods for establishing lines of effort, such as those already outlined in PPD-21. The sixteen critical infrastructure sectors identified by PPD-21 each hold its own line of effort and goals. The idea would be to establish these goals and compare them to see where the sectors overlap while combining or relating them to ensure that efforts are not duplicated and resources are efficiently used. The biggest goal of establishing a unified effort is to coordinate efforts and move away from the current and siloed methods being used by the different government agencies.

In order to improve resiliency and incorporate new ideas to streamline the improvement process, the gap between academia and government agencies enacting or creating policy to govern resilience must be closed. To accomplish this, specific requests for research information could be contracted out to academia. These requests should have the results specified and the research objectives should provide actionable and tangible results that community stakeholders can easily implement. Smart technologies and the positive effects that are possible from their application to resilience improvement projects must be identified and applied. Smart technology applications should have their own line of effort in order to ensure their inclusion in national policy.

Resiliency improvement is contingent upon the resiliency of individual entities within the system or network. The recommendation to incentivize private industrial sectors resilience and the improvement of different individual nodes of an infrastructure system is of great importance. If resiliency improvement policies can be applied to industry and infrastructure, then resiliency improvement policies can also be applied to social systems and individuals within a community. Education reform and programs should be incentivized to improve individual resilience. Programs that teach survival skills like swimming, first aid and outdoor survival should be incentivized to improve the community's resilience as a whole. Improving resilience and survival knowledge of individuals, families or neighborhoods could potentially ease the burden on emergency response personnel before, during and after the occurrence of a disturbance within a community. Social capital within communities can also be strengthened by time banking, community currency, focus group meetings, social events and planning of community layout and architectural structures. Improving social networks and ties in a community provides citizens with access to psychological support, information and physical resources that can be used to improve both disaster preparedness, emergency response and recovery. Strengthening social capital provides local, state and federal government agencies with another means of improving resilience outside the physical infrastructure resiliency improvement projects.

This thesis attempts to gather several literature reviews, theories, ideas and resiliency improvement tools in order to initiate the dialog for reforming or improving the current approach to resilience improvement and governance within the United States. The study is by no means an all-encompassing document and therefore will lead to further research which is required to enact some of the recommendations provided. This thesis is designed to be an overview of resilience by providing actionable recommendations for incorporation into future efforts regarding resiliency improvement strategies and policy making.

Bibliography

Adams, T. M., Bekkem, K. R., & Toledo-Durán, E. J. (2012). Freight resilience measures. *Journal of Transportation Engineering*, *138(11)*, 1403–1409. Retrieved from: https://doi.org/10.1061/(asce)te.1943-5436.0000415

Aldrich, D. P. (2012). Social, not physical, infrastructure: The critical role of civil society after the 1923 Tokyo earthquake. *Disasters*, *36(3)*, 398-419. Retrieved from: https://doi.org/10.2139/ssrn.1903911

Aldrich, D. P., & Meyer, M. A. (2015). Social capital and community resilience. *American Behavioral Scientist*, *59(2)*, 254–269. Retrieved from: https://doi.org/10.1177/0002764214550299

Aleksić, A., Stefanović, M., Arsovski, S., & Tadić, D. (2013). An assessment of organizational resilience potential in SMEs of the process industry, a fuzzy approach. *Journal of Loss Prevention in the Process Industries*, *26(6)*, 1238–1245. Retrieved from: https://doi.org/10.1016/j.jlp.2013.06.004

Allenby, B., & Fink, J. (2005). Toward inherently secure and resilient societies. *Science*, *309(5737)*, 1034–1036. Retrieved from: https://doi.org/10.1126/science.1111534

Arrow, K. J. (2000). Observations on social capital. In *Social capital: A Multifaceted Perspective*, 3–5. Washington, DC: World Bank.

Barrat, A., Barthelemy, M., Pastor-Satorras, R., & Vespignani, A. (2004). The architecture of complex weighted networks. In *Proceedings of the National Academy of Sciences, 101 (11),* 3747–3752. Retrieved from: https://doi.org/10.1073/pnas.0400087101

Bennett, B. (2007). *Understanding, assessing, and responding to terrorism.* Hoboken, New Jersey: Wiley. Retreived from: https://doi.org/10.1002/9781119237792

Bolar, A. A., Tesfamariam, S., & Sadiq, R. (2017). Framework for prioritizing infrastructure user expectations using Quality Function Deployment (QFD). *International Journal of Sustainable Built Environment*, *6(1)*, 16–29. Retrieved from: https://doi.org/10.1016/j.ijsbe.2017.02.002

Bouch, C. J., Rogers, C. D. F., Bryson, J. R., Quinn, A. D., Chapman, D. N., Barber, A. R. G., Jefferson, I., Coaffee, J., Williams, S., Chapman, L., Baker, C. J. (2012). Resistance and resilience – paradigms for critical local infrastructure. *Proceedings of the Institution of Civil Engineers - Municipal Engineer*, *165(2)*, 73–83. Retrieved from: https://doi.org/10.1680/muen.11.00030

Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., Shinozuka, M., Tierney, K., Wallace, W. A., Von Winterfeldt, D. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra*, *19(4)*, 733–752. Retrieved from: https://doi.org/10.1193/1.1623497

Cao, W., Cudney, H. H., & Waser, R. (1999). Smart materials and structures. *Proceedings of the National Academy of Sciences*, *96(15)*, 8330–8331. Retrieved from: https://doi.org/10.1073/pnas.96.15.8330

Carlson, J., Haffenden, R. A., Basset, G. W., Buehring, W. A., Collins III, M. J., Folga, S. M., Petit, F.D., Phillips, J.A., Verner, D.R., Whitfield, R. G. (2012). *Resilience: Theory and application*. Argonne, IL. Retrieved from: https://doi.org/10.2172/1044521

Chewning, L. V, Lai, C., & Doerfel, M. L. (2013). Organizational Resilience and using information and communication technologies to rebuild communication structures. *Management Communication Quarterly*, *27(2)*, 237–263. Retrieved from: https://doi.org/10.1177/0893318912465815

Clifton, C., & Duffield, C. F. (2006). Improved PFI/PPP service outcomes through the integration of alliance principles. *International Journal of Project Management*, *24(7)*, 573–586. Retrieved from: https://doi.org/10.1016/j.ijproman.2006.07.005

Cutter, S. L., Barnes, L., Berry, M., Burton, C., Evans, E., Tate, E., & Webb, J. (2008). A place-based model for understanding community resilience to natural disasters. *Global Environmental Change*, *18(4)*, 598–606. Retrieved from: https://doi.org/10.1016/j.gloenvcha.2008.07.013

Denecke, A. (2018). Federal investment in infrastructure: A mutually beneficial relationship | ASCE's 2017 Infrastructure Report Card. Retrieved from: https://www.infrastructurereportcard.org/federal-investment-in-infrastructure-a-mutually-beneficial-relationship/

Dinh, L. T. T., Pasman, H., Gao, X., & Mannan, M. S. (2012). Resilience engineering of industrial processes: Principles and contributing factors. *Journal of Loss Prevention in the Process Industries*, *25(2)*, 233–241. Retrieved from: https://doi.org/10.1016/j.jlp.2011.09.003

DOA / US. (2017). United States Army Field Manual: FM 3-0, 336. Retrieved from: https://fas.org/irp/doddir/army/fm3-0.pdf

Dunn, S., Fu, G., Wilkinson, S., & Dawson, R. (2013). Network theory for infrastructure systems modelling. In *Proceedings of the ICE-Engineering Sustainability, 166*, 281–292. Retrieved from: https://doi.org/10.1680/ensu.12.00039

Executive Order 13636 (2013). Improving critical infrastructure cybersecurity, *2(7)*. Retrieved from: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Fagiolo, G., Reyes, J., & Schiavo, S. (2010). The evolution of the world trade web: A weighted-network analysis. *Journal of Evolutionary Economics*, *20(4)*, 479–514. Retrieved from: https://doi.org/10.1007/s00191-009-0160-x

FDA, US Department of Health and Human Services, & Center for Food Safety and Applied Nutrition. (2019). Outbreaks - FDA continues investigation into source of E. Coli O157:H7 outbreak linked to Romaine lettuce grown in CA; CDC reports end to associated illnesses. Retrieved from: https://www.fda.gov/Food/RecallsOutbreaksEmergencies/Outbreaks/ucm626330.htm

Fisher, R. E., Basset, G. W., Buehring, W. A., Collins, M. J., Dickinson, D. C., Eaton, L. K., Haffenden, R.A., Hussar, N.E., Klett, M.S., Lawlor, M.A., Miller, D.J., Petit, F.D., Peyton, S.M., Wallace, K.E., Whitfield, R.G., Peerenboom, J. P. (2010). *Constructing a resilience index for the enhanced critical infrastructure protection program*. Argonne, Illinois.

Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety*, *121*, 90–103. Retrieved from: https://doi.org/10.1016/J.RESS.2013.07.004

Gilbert, S. W. (2010). Disaster resilience : A guide to the literature. *NIST Special Publication*, 125. Retrieved from: http://docs.lib.noaa.gov/noaa_documents/NOAA_related_docs/NIST/special_publication/sp_1117.pdf

Goble, G., Fields, H., & Cocciara, R. (2002). Resilient infrastructure: Improving your business resilience. *IBM*.

Goerger, S. R., Madni, A. M., & Eslinger, O. J. (2014). Engineered resilient systems: A DOD perspective. *Procedia Computer Science*, *28*, 865–872. Retrieved from: https://doi.org/10.1016/j.procs.2014.03.103

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet Of Things (IOT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29(7)*, 1645–1660. Retrieved from:

https://doi.org/10.1016/J.FUTURE.2013.01.010

Guha-Sapir, D., Hargitt, D., & Hoyois, P. (2004). *Thirty years of natural disasters 1974-2003: The Numbers.* Louvain-la-Neuve, Belgium: Presses Universitaires de Louvain. Retrieved from: https://doi.org/2930344717

Haimes, Y. Y. (2009). On the definition of resilience in systems. *Risk Analysis*, *29(4)*, 498–501. Retrieved from: https://doi.org/10.1111/j.1539-6924.2009.01216.x

Haimes, Y. Y., & Jiang, P. (2001). Leontief-based model of risk in complex interconnected infrastructures. *Journal of Infrastructure Systems*, *7(1)*, 1–12.

Hayajneh, A. M., Zaidi, S. A. R., McLernon, D. C., & Ghogho, M. (2016). Drone empowered small cellular disaster recovery networks for resilient smart cities. In *2016 IEEE International Conference on Sensing, Communication and Networking, SECON Workshops 2016*. Retrieved from: https://doi.org/10.1109/SECONW.2016.7746806

Healy, A., & Malhotra, N. (2009). Myopic voters and natural disaster policy. *American Political Science Review*, *103(03)*, 387–406. Retrieved from: https://doi.org/10.1017/s0003055409990104

Holler, J., Tsiatsis, V., Mulligan, C., & Karnouskos, S. (2014). *Internet Of Things*. Retrieved from: https://doi.org/10.1007/978-3-319-55405-1

Hollnagel, E. (2011). Prologue: The scope of resilience engineering. *Resilience Engineering in Practice: A Guidebook* (pp. xxix–xxxix).

Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. *Reliability Engineering and System Safety*, *145*, 47–61. Retrieved from: https://doi.org/10.1016/j.ress.2015.08.006

Klein, R. J. T., Nicholls, R. J., & Thomalla, F. (2003). Resilience to natural hazards: How useful is this concept? *Global Environmental Change Part B: Environmental Hazards*, *5(1)*, 35–45. Retrieved from: https://doi.org/10.1016/j.hazards.2004.02.001

Larkin, S., Fox-Lent, C., Eisenberg, D. A., Trump, B. D., Wallace, S., Chadderton, C., & Linkov, I. (2015). Benchmarking agency and organizational practices in resilience decision making. *Environment Systems and Decisions*, *35(2)*, 185–195. Retrieved from: https://doi.org/10.1007/s10669-015-9554-5

Li, C., Li, Q., Van Mieghem, P., Stanley, H. E., & Wang, H. (2015). Correlation between centrality metrics and their application to the opinion model. *European Physical*

Journal B, *88(3)*, 1–13. Retrieved from: https://doi.org/10.1140/epjb/e2015-50671-y

Longstaff, P. H., Armstrong, N., Perrin, K., Parker, W. M., & Hidek, M. A. (2010). Building resilient communities: A preliminary framework for assessment: Project on resilience and security white paper. *Homeland Security Affairs*, *4(3)*, 1–23. Retrieved from: http://www.hsaj.org/?fullarticle=6.3.6

Marcelo, D., Mandri-Perrott, X. C., House, S., & Schwartz, J. (2016). *Prioritizing infrastructure investment: A framework for government decision-making*. *World Bank Group*. Retrieved from: https://doi.org/10.2139/ssrn.2780293

McCrady, S. G. (2013). *Designing SCADA application software : a practical approach*. Elsevier. Retrieved from: https://books.google.com/books?id=_CDdZ55QxLsC&printsec=frontcover&dq=what+is+scada&hl=en&sa=X&ved=0ahUKEwi2p_XjueDaAhVI6IMKHfa_A2AQ6AEIKTAA#v=onepage&q=what is scada&f=false

McLeod, S. (2007). Certificate in counselling skills Maslow's hierarchy of needs, 3. Retrieved from: https://doi.org/10.1016/B978-0-88415-752-6.50250-2

McManus, S., Seville, E., Vargo, J., & Brunsdon, D. (2008). Facilitated process for improving Organizational Resilience. *Natural Hazards Review*, *9(2)*, 81–90. Retrieved from: https://doi.org/10.1061/(asce)1527-6988(2008)9:2(81)

Meerow, S., Newell, J. P., & Stults, M. (2016). Defining urban resilience: A review. *Landscape and Urban Planning*, *147*, 38–49. Retrieved from: https://doi.org/10.1016/j.landurbplan.2015.11.011

Mehta, A., Aggrawal, N., & Tiwari, A. (2016). Solar roadways-the future of roadways. *International Advanced Research Journal in Science, Engineering and Technology*, 2393–2395. Retrieved from: https://doi.org/10.17148/IARJSET

Minkel, J. R. (2008). The 2003 northeast blackout--five years later. *Scientific American*, *13*.

Morris, T., & Morris, T. V. (2004). *The stoic art of living: Inner resilience and outer results*. Open Court Publishing.

Mylrea, M., & Gourisetti, S. N. G. (2017). Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In *Proceedings - 2017 Resilience Week, RWS 2017*, 18–23. Retrieved from: https://doi.org/10.1109/RWEEK.2017.8088642

Nakagawa, Y., & Shaw, R. (2004). Social capital: A missing link to disaster recovery. *International Journal of Mass Emergencies and Disasters*, *22(1)*, 5–34.

Naoum, R. S., Abid, N. A., & Al-Sultani, Z. N. (2013). An enhanced resilient backpropagation artificial neural network for intrusion detection system. *International Journal of Computer Science and Network Security*, *13(3)*, 98–104. Retrieved from: http://paper.ijcsns.org/07_book/201203/20120302.pdf

Naqvi, S. A. R., Hassan, S. A., Pervaiz, H., & Ni, Q. (2018). Drone-aided communication as a key enabler for 5G and resilient public safety networks. *IEEE Communications Magazine*, *56(1)*, 36–42.Retrieved from: https://doi.org/10.1109/MCOM.2017.1700451

Norris, F. H., Stevens, S. P., Pfefferbaum, B., Wyche, K. F., & Pfefferbaum, R. L. (2008). Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness. *American Journal of Community Psychology*, *41(1–2)*, 127–150. Retrieved from: https://doi.org/10.1007/s10464-007-9156-6

O'Rourke, T. D. (2007). Critical infrastructure, interdependencies, and resilience. *BRIDGE-Washington-National Academy of Engineering*, *37(1)*, 365–386. Retrieved from: https://doi.org/10.1061/9780784412824.ch10

Ouyang, M., Dueñas-Osorio, L., & Min, X. (2012). A three-stage resilience analysis framework for urban infrastructure systems. *Structural Safety*, *36*, 23–31. Retrieved from: https://doi.org/10.1016/j.strusafe.2011.12.004

Ouyang, M., & Fang, Y. (2017). A mathematical framework to optimize critical infrastructure resilience against intentional attacks. *Computer-Aided Civil and Infrastructure Engineering*, *32(11)*, 909–929. Retrieved from: https://doi.org/10.1111/mice.12252

Pagano, A., Pluchinotta, I., Giordano, R., & Fratino, U. (2018). Integrating "hard" and "soft" infrastructural resilience assessment for water distribution systems. *Complexity*, 1–16. Retrieved from: https://doi.org/10.1155/2018/3074791

Panteli, M., & Mancarella, P. (2015). The grid: Stronger, bigger, smarter?: Presenting a conceptual framework of power system resilience. *IEEE Power and Energy Magazine*, *13(3)*, 58–66. Retrieved from: https://doi.org/10.1109/MPE.2015.2397334

Patent (1986). Pipeline built-in electric power generating set. Retrieved from: https://patents.google.com/patent/US4740711A/en

Patterson, S. A., & Apostolakis, G. E. (2007). Identification of critical locations across multiple infrastructures for terrorist actions. *Reliability Engineering and System Safety*, *92(9)*, 1183–1203. Retrieved from: https://doi.org/10.1016/j.ress.2006.08.004

Perrings, C., & Walker, B. (1997). Biodiversity, resilience and the control of ecological-economic systems : The case of fire-driven rangelands. *Ecological Economics*, *22*, 73–83. Retrieved from: https://doi.org/10.1016/S0921-8009(97)00565-X

Pfefferbaum, B. J., Reissman, D. B., Pfefferbaum, R. L., Klomp, R. W., & Gurwitch, R. H. (2007). Building resilience to mass trauma events. *Handbook of Injury and Violence Prevention*, 347–358. Retrieved from: https://doi.org/10.1007/978-0-387-29457-5_19

Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. *The International Journal of Logistics Management*, *20*. Retrieved from: https://doi.org/10.1108/09574090910954873

Postel, S. L. (2000). Entering an era of water scarcity: The challenges ahead. *Ecological Applications*, *10(4)*, 941–948. Retrieved from: https://doi.org/10.1890/1051-0761(2000)010[0941:EAEOWS]2.0.CO;2

Presidential Policy Directive 21 (2013). Critical infrastructure security and resilience. Retrieved from: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Ramiro, J., & Hamied, K. (2012). *Self-organizing networks : self-planning, self-optimization and self-healing for GSM, UMTS and LTE*. Wiley. Retrieved from: https://books.google.com/books?hl=en&lr=&id=i6Hute7zic0C&oi=fnd&pg=PT8&dq=p2p+self+healing+network&ots=PcCiTTeSkl&sig=QHbqC3c2D7KGp1yN0oePe0zz2xQ#v=onepage&q=p2p self healing network&f=false

Renschler, C. S., Frazier, A. E., Arendt, L. A., Cimellaro, G. P., Reinhorn, A. M., & Bruneau, M. (2010). Developing the "PEOPLES" resilience framework for defining and measuring disaster resilience at the community scale. In *Proceedings of the 9th US National and 10th Canadian Conference on Earthquake Engineering*, 25–29.

Rose, A. (2007). Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions. *Environmental Hazards*, *7(4)*, 383–398. Retrieved from: https://doi.org/10.1016/j.envhaz.2007.10.001

Schroeder, J. L., Demetsky, M., Friesz, T., & Yao, T. (2012). *Infrastructure Management Project A: Developing a framework for prioritizing infrastructure improvements on critical freight corridors Project B: Developing a market based framework for freight infrastructure management* (No. MAUTC-2010-01). United States. Dept. of Transportation. Research and Innovative Technology Administration.

Sheffi, Y., & Rice, J. B. (2005). A supply chain view of the resilient enterprise. *MIT Sloan Management Review*, *47(1)*, 41–49. Retrieved from: https://doi.org/10.1007/978-0-387-79933-9

Siisiäinen, M. (2000). Two concepts of social capital: Bourdieu vs. Putnam. *International Journal of Contemporary Sociology*, *40(2)*, 183–284. Retrieved from: https://doi.org/10.1083/jcb.200611141

Stephens, S. L., Collins, B. M., Biber, E., & Fulé, P. Z. (2016). U.S. Federal fire and forest policy: Emphasizing resilience in dry forests. *Ecosphere*, *7(11)*, 1–19. Retrieved from: https://doi.org/10.1002/ecs2.1584

Stewart, G. T., Kolluru, R., & Smith, M. (2009). Leveraging public-private partnerships to improve community resilience in times of disaster. *International Journal of Physical Distribution & Logistics Management*, *39(5)*, 343–364. Retrieved from: https://doi.org/10.1108/09600030910973724

Sun, Y., & Han, J. (2014). Ranking methods for networks. In *Encyclopedia of Social Network Analysis and Mining* 1488–1497. New York, NY: Springer New York. Retrieved from: https://doi.org/ISBN 978-1-4614-6170-8

Svendsen, N. K., & Wolthusen, S. D. (2007). Graph models of critical infrastructure interdependencies. In *IFPF International Conference on Autonomous Infrastructure, Management and Security,* 208–211. Springer, Berlin, Heidelberg. Retrieved from: https://doi.org/10.1007/978-3-540-72986-0_27

The Department of Homeland Security (2009). *Regional resiliency assessment*. Retrieved from: https://doi.org/10.1016/j.clinbiochem.2006.09.001

The Department of Homeland Security (2013). NIPP 2013: Partnering for critical infrastructure security and resilience. *Homeland Security*, 57. Retrieved from: https://doi.org/10.1017/CBO9781107415324.004

The Department of Homeland Security (2019). Our mission homeland security. Retrieved from: https://www.dhs.gov/our-mission

The Joint Chiefs of Staff (2014). *Joint Publication 3-13: Information Operations*.

Washington D. C.

The Merriam-Webster Dictionary (2019) Resilience. Retrieved from: https://www.merriam-webster.com/dictionary/resilience

The US Army Corps of Engineers (2016). *EP 1100-1-2: USACE Resilience Initiative Roadmap*. Washington D. C.

Ting, M. M. (2003). A Strategic theory of bureaucratic redundancy. *American Journal of Political Science*, *47(2)*, 274–292. Retrieved from: https://doi.org/10.1111/1540-5907.00019

Türk, A. (2013). Failure to act. *Judicial Review in EU Law*. Retrieved from: https://doi.org/10.4337/9781848447493.00008

Tusaie, K., & Dyer, J. (2004). Continuing education resilience: A historical review of the construct, *Holistic Nursing Practice,18(1),* 3–10.

US Marines. (2019). US Marines Training Command. Retrieved from: https://www.trngcmd.marines.mil/Portals/207/Docs/wtbn/MCCMOS/Planning Templates Oct 2017.pdf?ver=2017-10-19-131249-187

Vugrin, E. D., & Camphouse, R. C. (2011). Infrastructure resilience assessment through control design. *International Journal of Critical Infrastructures*, *7(3)*, 243. Retrieved from: https://doi.org/10.1504/ijcis.2011.042994

Walden, J. (2011). Comparison of the STEEPLE strategy methodology and the Department of Defense’s PMESII-PT methodology. *Supply Chain Leadership Institute*, 1–14.

Wang, Z., Scaglione, A., & Thomas, R. J. (2010). Electrical centrality measures for electric power grid vulnerability analysis. In *49th IEEE Conference on Decision and Control (CDC),* 5792–5797. Retrieved from: https://doi.org/ISBN 978-1-4244-7745-6

Weijnen, M. P., & Bouwmans, I. (2006). Innovation in networked infrastructures. *International Journal of Critical Infrastructures*, *2(2/3)*, 121–132.

Xu, N. (2002). A survey of sensor network applications. *Energy*, *40(8)*, 1–9. Retrieved from: https://doi.org/10.1.1.131.9647

Yodo, N., & Wang, P. (2016). Engineering resilience quantification and system design implications: A literature survey. *Journal of Mechanical Design*, *138(11)*, 111408. Retrieved from: https://doi.org/10.1115/1.4034223

Zhang, Z. (2018). Class notes. In *CE392N(2) Infrastructure Management*. Austin, TX.

Vita

Vita

Captain Promotable (CPT (P)) John Charles Collier was raised in Virginia, where he attended Woodberry Forest School and the Virginia Military Institute (VMI). He holds a Bachelor of Science in Civil Engineering, graduating with Honors and as a Distinguished Military Student in May 2009. CPT Collier was commissioned as an Engineer Officer and attended the Basic Officer Leader Course at Ft Sill, Oklahoma and the Engineer Officer Basic Course at Ft Leonard Wood, Missouri.

CPT Collier was assigned to the 7th Engineer Battalion (EN BN) (CBT) at Fort Drum, NY. There he served as a Platoon Leader (PL) in the 630th Route Clearance Company (RCC), Executive Officer (XO) for the 642nd Engineer Support Company (ESC), and Assistant S-3 Counter-Improvised Explosive Device (CIED) Officer. CPT Collier deployed to Southern Afghanistan as a Route Clearance Platoon Leader from February to July of 2010, and to Eastern Afghanistan as an XO and CIED officer from November 2011 to November 2012.

In January 2013, CPT Collier attended the Special Forces Assessment and Selection Course and was selected to attend the Special Forces Qualification Course (SFQC) at Fort Bragg, NC. March 2013 to June 2013, he completed the Special Operation Forces Officer Common Core Course (SOFCCC). Following SOFCCC, CPT Collier achieved a 1+/1+ in Mandarin Chinese on the Oral Proficiency Interview (OPI) and graduated from Small Unit Tactics (SUT) course, and Survival, Escape, Resistance and Evasion (SERE-C) training.

Vita

CPT Collier was assigned to the 307th EN BN at Fort Bragg, NC in December 2014 and immediately deployed to Iraq from January to September 2015. During this deployment, he partnered with three Iraqi Brigadier Generals as the 307th EN BN's Security Force Advise and Assist Team (SFAAT) Engineer, Training, and C-IED Advisor to the Baghdad Operations Command (BOC).

Upon redeploying from Iraq, CPT Collier was assigned as the Assistant Operations Officer for Training in the 307th EN BN. During this time CPT Collier was the Honor Graduate of the 82nd Airborne Division's Pre-Ranger Course in December 2015 and graduated from Ranger School in March 2016. CPT Collier also graduated from Jumpmaster School in May 2016. June 2016 to December 2017 CPT Collier commanded B/307th Sapper Company. Since January 2018 CPT Collier has been assigned as an advanced civil schooling graduate student at the University of Texas at Austin to pursue a Master's degree in Civil Engineering, Transportation Engineering.

Permanent email: collierjc127@gmail.com

This dissertation was typed by John C. Collier.