8-2014

Legislative and Policy Issues Hindering Resilience of Critical Infrastructure and Key Resources against Cyber Threats

Jesse A. Magenheimer

School of Public Service and Health

Emergency and Disaster Management

The thesis for the master's degree submitted by

Jesse Magenheimer

under the title

Legislative and Policy Issues Hindering Resilience of
Critical Infrastructure and Key Resources against Cyber Threats

has been read by the undersigned. It is hereby recommended for acceptance by the faculty with credit in the amount of three semester hours.

Christina Spoons, Ph.D. Date: June 16, 2014
Randall G. Cuthbert, Ph.D., Reader
Recommended for approval on behalf of the program

Terri L. Wilkin, J.D. Date: June 17, 2014
Terri L. Wilkin, J.D. Program Director
Recommendation accepted on behalf of the program director

Date: June 17, 2014
Constance St. Germain, Esq., Dean
Approved by Academic Dean

LEGISLATIVE AND POLICY ISSUES HINDERING RESILIENCE OF CRITICAL INFRASTRUCTURE AND KEY RESOURCES AGAINST CYBER THREATS

A Master Thesis

Submitted to the Faculty

of

American Public University

by

Jesse Magenheimer

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Arts

June 2014

American Public University

Charles Town, WV

DEDICATION

I dedicate this thesis to my family. They have supported and encouraged me throughout this journey—even when my studies took me away from familial commitments—and for that I am grateful.

I also dedicate this thesis to my best friend, Bradley Michael Smith. His academic achievements and goals inspired me to pursue my graduate degree in the field of Emergency Management. He has been an unwavering source of professional mentorship and the most loyal friend for which a person could ever hope.

ACKNOWLEDGMENTS

I wish to thank my professors—especially Dr. James Smith (ret.), Dr. Randall Cuthbert, and Dr. Chris Spoons. Their detailed, critically constructive feedback and coaching has made me a better contributing member to the academic community. Dr. Chris Spoons helped me take an idea of great interest and craft it into a meaningful thesis by guiding and encouraging me throughout the admittedly daunting process.

Lastly, I wish to thank my colleagues who continue to challenge me through critical discourse and exciting work assignments while affording me opportunities to grow as a professional. I am truly honored to work with such a talented and inspiring team.

ABSTRACT OF THE THESIS

LEGISLATIVE AND POLICY ISSUES HINDERING RESILIENCE OF CRITICAL INFRASTRUCTURE AND KEY RESOURCES AGAINST CYBER THREATS

by

Jesse Magenheimer

American Public University System, June 22, 2014

Charles Town, West Virginia

Professor Christina Spoons, Thesis Professor

This research addresses the importance of cybersecurity resilience for critical infrastructure and key resources for emergency managers in their communities. The issue is framed by the relevance for practitioners, the challenging legal and policy landscape, and the criticality of the public-private sector dynamic in achieving greater resilience against cyber threats. Leveraging a qualitative research methodology, the findings and recommendations affirm the salience of the topic for emergency managers. Incongruent policy and legislation coupled with insufficient collaboration between the public sector and private sector owners of critical infrastructure requires emergency managers to draw upon their knowledge, skills, and abilities as they seek to address the issue in their planning and preparedness efforts.

TABLE OF CONTENTS

Legislative and Policy Issues Hindering Resilience of Critical Infrastructure and Key Resources against Cyber Threats

Emergency management remains an evolving discipline with much of its focus and advancement precipitated by the relatively recent events of September 11, 2001 and the devastation from Hurricanes Katrina and Rita in 2005. The body of knowledge for practitioners and academics continues to grow—especially in the areas of emerging hazards and their associated vulnerabilities. Although emergency managers are skillful at coordination, their work is by no means singularly focused on a specific topic or issue. Successful emergency managers excel at a multitude of challenges and adapt to incorporate new knowledge and perspectives as the profession continues to develop in many different ways.

Historically, emergency managers have spent much of their time mitigating, preparing for, responding to, and aiding in the recovery from emergencies or disasters of both a natural or human-made nature. With the formalized intentional expansion and recognition of the homeland security discipline in 2002, emergency management shifted focus slightly to increase emphasis on terrorism. Even with the addition of the terrorism mandate in various laws and policies, the emergency management discipline remains heavily grounded in the physical side of the world. And, admittedly, that is where many emergency management advancements and maturation must still occur. Communities still need to prepare for floods, chemical leaks, mass casualty event, or a myriad of other possible issues that could present an emergency or disaster.

Yet, hazards will by no means slow and conveniently wait for those working to manage them to catch up. Hazards will continue to expand and evolve into new challenges that emergency managers must begin to understand and incorporate into their already expansive planning and operational practices. While the physical world presents ongoing unique problem

sets that fall within an emergency manager's purview, the issues developing in cyberspace promise to test practitioners and academics within the discipline as well as adjacent fields of study in new or different ways. Though the societal reliance on technology and the virtual space enabled from the Internet are quite established at this point, the threat landscape in that regard shifts very quickly and the collective understanding in this landscape as well as the applicable legislation and policy consistently struggles to keep pace with the changes.

The American society has a penchant to take many of its service and technological experiences for granted. For instance, there is rarely a question that power will be available when a light switch is activated in a home or office. Depressing the button at a water fountain consistently delivers safe, potable water. Depositing money in a bank account rarely results in those funds incorrectly being applied to a different account. And accessing the Internet from a traditional or mobile device for near real-time news, sports, weather, or business purposes is almost a natural daily activity for nearly 72 percent of American households (U.S. Census Bureau, 2013). Clearly, reliance on critical infrastructure such as electrical services, water treatment and delivery, financial transactions, and telecommunications have become vital to daily societal activities in the United States. It is equally apparent that the Internet is an integral component of a vast majority of Americans' lives based on the most recent U.S. Census data (U.S. Census Bureau, 2013).

Herein lies the convergence of the physical world with cyberspace that must become a priority focus for emergency managers and all levels of government. The Internet extends benefits well beyond the casual user in that it has enabled businesses and governments alike to gain efficiencies and expand their capabilities through its expansive connectedness. Vital services such as power delivered through electrical grids, water treatment and delivery,

communications, investment and banking transactions, and transportation control have become connected to the Internet in ways that allow for remote management and monitoring and, in some cases, expand the availability of services to end users. These resources are so vital to the stability and security of the nation that they have been designated as critical infrastructure/key resources (CI/KR) by the United States government (Obama, 2013). Cyber attacks against these resources as a result of their connectedness via the Internet would be substantial in the best case and potentially disastrous in the worst case (Singer & Friedman, 2013). Results of such attacks will not be confined to cyberspace; rather, they have the very real potential to manifest impacts in the physical world (Singer & Friedman, 2013). Thus, these systems, which can feasibly be attacked from any connected endpoint on the Internet, must demonstrate high levels of resilience through robust cyber security measures.

Emergency managers do not have the luxury of ignoring the viable cyber threat in their mitigation, preparedness, response, and recovery responsibilities. While they need not become cyber security experts themselves, they must incorporate the threat vectors introduced in this regard in their greater plans for CI/KR in the communities in which they serve. As a report by Clayton (2011) in the Christian Science Monitor states, “In the future, wars… will also be fought with the click of a mouse a half a world away that unleashes carefully weaponized computer programs that disrupt or destroy critical industries like utilities, transportation, communications, and energy” (as cited in Singer & Friedman, 2013, p. 1). Therefore, in their efforts to advance the protection of their communities from the outcomes of a cyber attack on their CI/KR, emergency managers must also become familiar with the salient legislative mandates, enabling policies, and the incongruences that currently exist in both at the federal level in order to bridge the public-

private sector divide hindering optimal resilience and advocate for changes that improve the current status quo.

This thesis sought to address the following research questions.

1. What cyber threats face CI/KR and how do those threats relate to the work of emergency managers?
2. What legislative and policy challenges exist that hinder greater advancement of resilience for CI/KR against cyber attacks?
3. How do legislative and policy gaps translate to public and private sector dynamics?
4. What recommendations are pertinent for emergency managers given the findings that will help them further resilience against cyber threats to critical infrastructure and key resources?

The remainder of this document addresses the literature that comprised the body of the research conducted in pursuit of answering the questions above, the findings rendered from a qualitative analysis of the literature, recommendations for addressing the issues that emerged in the data analysis, and questions or problems that warrant future academic research.

Literature Review

Understanding Critical Infrastructure and Key Resources

As alluded to in the problem statement, CI/KR is vital to both the immediate and long-term stability of the United States and therefore deemed a national security interest at the federal level. Following the terrorist attacks of September 11, 2001, greater recognition as to the potential vulnerabilities of sectors such as energy, telecommunications, water and waste management, and transportation systems occurred within the intelligence, emergency management, and homeland security communities. Mandates regarding the definition and

protection of these resources became codified in laws later in 2001 through the USA PATRIOT Act and in 2002 in the Homeland Security Act. While the importance of these resources may now seem rather obvious, very few formal specifications prior to the terrorist attacks on September 11, 2001 existed to clearly articulate what constituted such a resource, designate responsibilities for oversight, and establish a legislative impetus for protection.

Several pieces of legislation or policy comprise the body of information pertinent to CI/KR. First, referring to the USA PATRIOT Act of 2001, it states that critical infrastructure constitutes "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (USA PATRIOT ACT, 2001). It is important to note the intentional inclusion of CI being either physical or virtual in this definition as that not only provides a valuable qualifier, it can also indicate the possible origins of threats in either space. Secondly, the Homeland Security Act of 2002 offers a definition of key resources as "publicly or privately controlled resources essential to the minimal operations of the economy and government" (Homeland Security Act, 2002). Together, both legislative acts lay a foundation for conceptually the systems and resources that, if negatively affected, would result in severe life safety consequences as well as detrimental impacts to the country's security, financial stability, and overall operations.

Additionally, several sections of the United States Code provide applicable legislative mandates and authorities for the protection of CI/KR. 6 U.S.C. §§121-122 (2006) consists of subsections entitled Directorate for Information Analysis and Infrastructure Protection and Access to Information, respectively. The first subsection clearly establishes a directorate within the Department of Homeland Security (DHS) that is responsible for enabling the protection of

critical infrastructure and analyzing information that furthers protection efforts. It discusses the associated staffing authorized to lead the directorate and charges the organization with assessment and policy recommendations as well as the development and maintenance of a national plan to secure critical infrastructure/key resources (CI/KR). The second subsection authorizes the Secretary of the DHS to have access to threat and vulnerability information as well as other information germane to infrastructure protection.

6 U.S.C. §§131-133 (2006), consists of subsections entitled Definitions, Designation of Critical Infrastructure Protection Program, and Protection of Voluntarily Shared Critical Infrastructure Information. The first two subsections are administrative in nature but offer applicable definitions pertinent to the CI/KR legislative landscape as well as authorities for the President and Secretary of the DHS. The third subsection addresses handling of voluntarily provided CI information to a government agency. It is meant to offer assurances to CI owners (typically private sector firms) that their information will be protected if submitted in the hopes of fostering collaboration.

Added in 2007, 6 U.S.C. §321m is entitled Voluntary Private Sector Preparedness Accreditation and Certification Program. This subsection mandates designation of a government officer that shall partner with highly qualified nongovernmental entities to develop voluntary consensus standards for critical infrastructure. Additionally, the subsection charges the Secretary of the DHS with implementing voluntary accreditation and certification programs for the private sector. Lastly, 6 U.S.C. §§441-444 (2006) consists of subsections that deal with the support of anti-terrorism by fostering effective technologies to combat terrorism (including information technologies). It addresses the administrative aspects of this subject matter as well as litigation and risk management components. These subsections demonstrate that the federal government

has a stated interest in the development of technologies that can protect CI/KR from cyber attacks. Interestingly, another source referenced later in the literature review will indicate that the federal government does not specifically protect commercial networks. Given the legislative interest noted herein and the conflicting claim in the later peer-reviewed journal publication, one can immediately observe the incongruent legislative and policy landscape issues that will be more fully addressed throughout subsequent sections of the literature review.

Providing more specific expectations for CI/KR protection beyond the definitional content of either of the aforementioned acts and the pertinent sections of the United States Code, President George W. Bush released Homeland Security Presidential Directive 7 (HSPD-7) in December 2003 (DHS, 2013b). HSPD-7 was superseded in 2013 by Presidential Policy Directive 21, which sought to "[advance] a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure" (Obama, 2013, p. 1). This policy directive revised the number of critical infrastructure sectors from 18 under HSPD-7 to 16 and established, among other things, sector-specific agencies (SSAs) that are on point for the respective assigned sector(s) (DHS, 2013a). Presidential Policy Directive 21 established the following critical infrastructure sectors

- chemical;
- commercial facilities;
- communications;
- critical manufacturing;
- dams;
- defense industrial base;
- emergency services;

- energy;
- financial services;
- food and agriculture;
- government facilities;
- healthcare and public health;
- information technology;
- nuclear reactors, materials, and waste;
- transportation systems; and
- water and wastewater systems (Obama, 2013, p. 10-11).

It should be apparent from the listed critical infrastructure sectors that few, if any, exist in isolation. What this means is that a disruption or attack to one sector has the real likelihood of adversely impacting other critical infrastructure sectors or associated key resources (DHS, 2013c). The National Infrastructure Protection Plan (NIPP) recognizes that attacks using components of the nation's CI/KR can go well beyond physical impacts in that there may well be a psychosomatic aftermath that accompanies the attack (DHS, 2013c). A loss in confidence as to the surety of the very systems intended to provide for the population's well-being and way of life can certainly inspire the level of terror often being sought by organizations grounded in terroristic ideals. Both the NIPP and Presidential Policy Directive 21 acknowledge and compel stakeholders in the intelligence, emergency management, homeland security, and other closely aligned communities to take real and measurable action that achieves expected levels of resilience to minimize the potential catastrophic outcomes that could arise from an attack against CI/KR.

As should be evident, the previously covered legislative and policy components provide the applicable context for the importance of CI/KR as well as the significant impetus for its protection and resilience. Many of these legislative and policy items should be very familiar to emergency management practitioners as they comprise some of the core elements of the contemporary discipline. The aforementioned acts and policies are also mainstays in various emergency management higher education literature such as texts by Sylves (2008), Haddow, Bullock, and Coppola (2011), and Hunter (2009). Together, the policies and legislation discussed work in tandem to drive much of the protection and resilience activities deemed necessary for the safety of these critical assets.

Contemporary Cyber Threat Issues and the Implications for CI/KR

President Obama stated in his May 2009 Cyberspace Policy Review that "cybersecurity risks pose some of the most serious economic and national security challenges of the 21st century" (Singer and Friedman, 2013, p. 1). In his 2014 speech at the RSA Conference in San Francisco, FBI Director James Comey indicated that cybersecurity is again at the top of the Director of National Intelligence James Clapper's list of threats that face the United States—outranking terrorism, espionage, and weapons of mass destruction for the second year straight (Comey, 2014). During his confirmation hearing for the position of Secretary of Defense in 2011, Leon Panetta argued to the confirmation committee that the "next Pearl Harbor that we confront could very well be a cyber attack that cripples our power systems our grid, our security systems, our financial systems, and our governmental systems" (Glick, 2012, p. 101). Echoing a similar message, Senator Jay Rockefeller has indicated that a significant cyber attack has the real potential to adversely affect critical infrastructure including power grids, telecommunications systems, and the banking and financial services sectors (Glick, 2012).

The past five years have seen a flurry of activity in the cybersecurity realm as new and complex threats emerge. Complicating the security topic further is the ongoing growth of online-enabled systems and access to the Internet from more parts of the world than ever before. Singer and Friedman (2013) stated that an estimated 8.7 billion devices were connected to the Internet by the end of 2012 and that the number will continue to rise significantly in the next decade to well over 40 billion. In developed countries, businesses run a very real risk of failing without an Internet presence and most of the business transactions and supporting administrative functions that occur in today's current environment require high-speed Internet access. Unfortunately, statistics are not flattering when it comes to cybersecurity breaches among some of the biggest companies around the world. Of the existing companies ranked in the Fortune 500, 97 percent have been hacked (Singer & Friedman, 2013). This signals a legitimate threat to the cybersecurity of systems connected to the Internet and further substantiates the need for cyber resilience in CI/KR.

Singer and Friedman (2013) have described cybersecurity as a "wicked" problem. Cybersecurity as a wicked problem consists of properties identified by Rittel and Webber (1973) in that there are tradeoffs—both positive and negative—to be had with any solution and that the issue has no stopping rule that signals when the problem has been resolved. It can be further argued based on the criteria by Rittel and Webber (1973) for wicked problems that cybersecurity as a problem is a symptom of other social problems. People are at much of the root of the cybersecurity dilemma (Singer & Friedman, 2013) and this makes reliance solely on technical controls an inadequate security proposition. It will be demonstrated in later content of this thesis that this social challenge is at the root of much of the current cybersecurity issues requiring overall improvement for optimal resilience.

Cyber threats to critical infrastructure can originate from several sources. A rather unlikely origination of such attacks comes from traditional script kiddies who first rose to greatest prominence in the early days of the expansion of the World Wide Web (Kelly & Hunker, 2012). These are generally unsophisticated individuals who lack depth of knowledge in either computing systems and/or malicious hacking techniques. Rather, they rely heavily on scripts or tools developed by others to launch targeted attacks against systems. Motivations generally arise from a desire to outsmart security controls and not for financial gain or terroristic intentions.

More targeted attacks are emerging from hactivist organizations around the world. “Hactivism refers to the marriage of hacking and activism. It covers operations that use hacking techniques against a target's Internet site with the intent of disrupting normal operations but not causing serious damage” (Arquilla & Ronfeldt, 2001, p. 241). In recent years, the financial services sector has particularly drawn the ire of hactivist groups and, as a result, large attacks have occurred against very prominent financial organizations such as Visa, Mastercard, and PayPal as well as some of the biggest banks in the world (MacCarthy, 2012; Kelly & Hunker, 2012). A prominent and contemporary form of political hactivism that jeopardized national security was the 2010 WikiLeaks publication of stolen U.S. government cables (Kelly & Hunker, 2012). Consequences for the WikiLeaks publication and subsequent denial of service (DOS) actions that occurred from unknown groups involved political hactivists launching retaliatory attacks against U.S. government sites.

While hacktivists and script kiddies have played a role in various detected hacking events over the years, these two populations remain a relatively minor threat vector when compared to that of organized crime, terrorists, and nation states. This latter category is perhaps the most

threatening to the resilience of CI/KR because of the resources and capabilities available to such groups. Attacks such as the Diginotar compromise in the Netherlands against 300,000 Iranian Gmail users, the Titan Rain attacks against American computer systems, or the Stuxnet worm targeting Iranian nuclear enrichment centrifuges reflect advanced capabilities utilized against not individuals or organizations, but governments (Daskapan & van den Berg, 2011). Vasilescu (2012) posits "China is the state presumably to be one of the most active and most interested in [cyber attacks], along with Israel, India, Pakistan and the United States" (p. 57). Recalling Clayton's (2011) statement that future wars may transcend the physical space into the virtual space by targeting control systems for CI/KR, such an attack would be most advantageous for nation states through either hired organized crime to hide the true source or via covert military action by ensuring traceability to the source cannot be determined.

The Stuxnet worm warrants further discussion since it is a very contemporary instance of specific physical-world infrastructure being targeted in an attack to cause real, substantial damage. In 2010, cyber security experts around the world were observing a malicious worm moving throughout the Internet inserting itself into supervisory control and data acquisition (SCADA) systems (Singer & Friedman, 2013; Kelly & Hunker, 2012). The worm had been predominately attacking centrifuge systems used for Uranium enrichment in the Iranian nuclear fuel refinement program (Kelly & Hunker, 2012). It attacked a specific software system, the Siemen's WinCC/PCS 7 SCADA control software, which was used in Iran's case to control the intricate operations of the enrichment centrifuges (Singer & Friedman, 2013). With the worm disrupting centrifuge speeds and timing, the enrichment of the Uranium for potential nuclear bomb creation (Kelly & Hunker, 2012) failed and the Uranium was rendered unusable as nuclear

fuel. “This event was the first tangible illustration that cyber attacks can disrupt not just computers, but also physical processes in the real world” (Kelly & Hunker, 2012, p. 211).

What sets Stuxnet apart from other malicious worms observed to that point was the nature of the program itself. Upon dissection, the code revealed four “zero day” exploits that were previously unknown in the cyber community (Singer & Friedman, 2013). The code also showed incredible versatility to operate on every Microsoft Windows operating system back to 1995. The nature of specificity in the code is what particularly raised the bar on this malicious worm when compared to previously observed malware in the wild. It had controls within it to attack the Siemen’s software noted above and further controls to render itself inert if the software was not present on the target host (Singer & Friedman, 2013). It would appear the worm was developed with a specific intent and its creators sought to keep it from doing damage beyond its specific targets, which were predominately Iranian nuclear centrifuges. Cybersecurity expert Ralph Langner, in his analysis of Stuxnet, indicated the method of attack employed in this worm was “as good as using explosives” to attack the targeted enrichment facilities (as cited in Singer & Friedman, 2013, p. 116). The insidious way in which Stuxnet exploited trust in the physical systems and not the computers through which the worm was inadvertently introduced signals a highly covert and well-funded form of warfare translated from theory to practice and reinforces the potential of what dangers await other CI/KR in terms of cyber attacks. Most notably, according to Singer and Friedman (2013), it was later leaked that the Stuxnet worm was a joint covert development between the United States and Israel. This revelation very much affirms what for years has been suspected: Nation states are leveraging cyber attacks as a way to wage wars on a new front without the need for traditional military assets.

The previous example sets the tenor for what attacks against CI/KR can entail. One may initially conclude that such attacks would be visible, possibly involving immediate threats to life safety in a physical sense. However, cyber attacks on CI/KR can be just as detrimental in other ways without inflicting direct loss of life, injuries, or damage to facilities or other assets. For instance, impacting CI/KR in a community may render the CI/KR inoperable, in turn affecting jobs, morale, quality of life, and potentially the financial stability of the region. Attacks may disrupt productivity to such a detrimental extent that others relying on outputs from critical manufacturing or other vital services may be without those products and services when most needed (i.e. biomedical products, parts for key water treatment systems in communities). Core telecommunications systems may fail during cyber attacks, thus taking down 911 services, military coordination systems, and air traffic control capabilities, which could jeopardize the lives of thousands.

Attacks against CI/KR can manifest in many ways. According to Genge, Siaterlis, and Hohenadel (2012), today's critical infrastructure for power plants, water treatment and distribution systems, and smart grids utilize systems referred to as Information and Communication Technologies (ICT). Benefits of ICTs are numerous in that they offer "cost optimization as well as greater efficiency, flexibility and interoperability between components" (Genge, Siaterlis, & Hohenadel, 2012, p. 673). Networked Industrial Control Systems (NICS) are a form of ICTs and draw on the fact that they are connected via a common backbone at some point to leverage the benefits noted above. The aforementioned SCADA systems become components of NICS when connected through the Internet or privately managed, independent networks. As observed with Stuxnet, one attack vector involves the modification of processes controlled by SCADAs so that the physical operations break down or fail to operate as designed.

This can be one of the most insidious forms of attack against CI/KR since it reveals itself in multiple places throughout the CI/KR operational chain. Other vectors, however, also exist including distributed denial of service (DDoS) attacks in which thousands of compromised systems overwhelm the entry points into private networks with SCADA systems attached or flood the SCADA systems directly (Genge, Siaterlis, & Hohenadel, 2012). The systems become unavailable for remote or possibly local management as a result and could certainly jeopardize life safety of a community should this become a reality. Attacks may also involve information operations with the intent to "further disrupt, demoralize and confuse" (Miller, 2011, p. 84). For instance, envision improper purification at water treatment plants that distribute water to millions of consumers. Entire cities may fall ill as a result and the necessary pandemic response would take time and resources to determine the origins of the illness before beginning to investigate the underlying purification and treatment systems and their associated control subsystems.

Other attack scenarios against CI/KR should be equally evident to emergency managers as impacting the communities in which they serve. Consider the disruption of telecommunications and IT networks that subsequently cause the failure of 911 call systems as well as emergency responder dispatching. Attacks affecting power plants in local communities may in the best case result in power failure if the plant is a supplier to the community itself or, in the worst case, explosions or meltdowns of systems requiring evacuation and likely resulting in a mass casualty incident. Malicious attacks on air traffic control systems can place community members in harm should airplanes in the sky lose coordination with ground control towers. As noted previously, the financial stability of a community, region, or the nation itself could be adversely affected as well if the financial and banking system was the victim of a coordinated cyber attack. Despite these few examples, it should be apparent that emergency managers have a

stake in the cybersecurity of their community's CI/KR and must begin to understand the threat landscape, advocate for greater resilience, and incorporate the threats into their regular planning and preparedness efforts.

As a final observation, the American Public University System's Emergency and Disaster Management graduate program recently added a course entitled "Emergency Management Perspectives on Cybersecurity" (APUS, n.d.). The course description indicates that resilient cyber infrastructure is foundational to emergency and disaster management and is critical to enabling effective response during natural disasters, terrorist attacks, and other public safety issues (APUS, n.d.). Emphasis is placed on infrastructure impact awareness as a core component of the cybersecurity topic in addition to communication and deterrence. Creation of such a course signals the growing salience of the topic for both emergency management practitioners and academics and further substantiates the claim herein that emergency managers, from a diligence and duty to act perspective, must begin to incorporate this topic into their broader efforts. Admittedly, this is a multi-threaded topic that cannot fall to local emergency managers alone. State and federal programs play equally critical roles and, as will be evident in later sections of the literature review, incongruences in legislation and policy at the federal level in particular will present very noticeable challenges for the state and local practitioners.

Threat Assessment Complications Affecting Risk Quantification

Emergency managers must be good risk managers and the cybersecurity threat against CI/KR poses some interesting complications when it comes to effectively understanding aspects of the standard risk equation of *risk = threat x vulnerability x cost* (DHS, 2011). The previous section of the literature review addressed many aspects around the vulnerability of CI/KR to cyber attacks and further touched on conceptual cost impacts at a high level. However, the threat

multiplier in the risk equation is recognized as a difficult factor to quantify for several reasons. The intent of this section of the literature review is to draw upon some of the documented difficulties in establishing accurate cyber attack threat assessments and how that complicates the broader work that emergency management practitioners must do when attempting to incorporate cybersecurity into their ongoing efforts.

Chittister and Haimes (2011) found that the risks related to cyber attacks on CI/KR are dependent on both the resilience of the system(s) in question and the erudition of any given attack itself. Attacks against CI/KR via cyber systems are probabilistic in nature while the consequences are "functions of the vector states of the cyberinfrastructure system" (Chittister & Haimes, 2011, p. 6). Approximately 90 percent of the CI/KR in the United States is owned by the private sector (Singer & Friedman, 2013), yet the government arguably has a stake in its resilience and security. As generally for-profit entities, owners and managers of CI/KR must weigh the explicit and implicit tradeoffs associated with mitigation and resilience for their infrastructure against the costs of doing so from a business perspective. While private sector entities have a very real impetus to invest in the resilience and security of their systems against cyber attacks, the degree to which they do so (as a function of the likelihood of future attacks when such quantification is probabilistic and inexact) is difficult to ascertain. Emergency managers will be challenged in influencing this as well because the threat assessment process that should give insight into the likelihood and feasibility aspects faces documented issued.

Whereas physical capabilities and assets, especially those of nation states, are often ascertainable through intelligence gathering, the same cannot be said for cyber capabilities. When considering cyber assets and abilities, "hardware and software determine the landscape of the battlefield, not mountains, valleys, or waterways. The most formidable obstacles, and the best

offensive and defensive tactics, are usually not the most physically imposing, but the most logical and innovative" (Geers, 2010, p. 125). The pervasiveness of the Internet has somewhat leveled the warfare playing field if attacks occur via cyberspace. Vast military assets and staffing used to be an indicator of a nation state's security posture along with the physical landscape benefits afforded by the nation state itself. Given the broad access to hardware and software that is readily available in today's global market as well as the connectedness afforded through the Internet, many nation states could be argued to possess comparable cyber warfare capabilities (Lin, 2012).

In the physical world, risk-based decisions grounded in adversarial intent tend to be more indeterminate and speculative than similar decisions rendered based on adversarial capabilities (Lin, 2012). The same cannot be said for risk-based decisions relying on adversarial capabilities regarding cyber weapons (Lin, 2012). This is because cyber abilities and associated weapons more closely share similarities to thought than to material objects—the often key physical items upon which capabilities are ascertained. Because of this, threat assessments for cyber attacks and adversarial capabilities are problematic in that they struggle to accurately quantify the actual threat for policymakers and public safety practitioners.

More specifically, threat assessments in both the physical world and the logical space are more pre-disposed to be overestimated in conveying worst-case scenarios associated with a given threat when the analysis upon which they are based involves minimal or incomplete data about adversarial capabilities (Lin, 2012). Lin (2012) points to this practice being a key component that influences worst-case analysis in threat assessment reporting by intelligence agencies. "When they focus only on capabilities, analysts omit the adversary's operational skill (also known as tradecraft) from the scope of their analysis and necessarily assume that the adversary will not

make mistakes" (Lin, 2012, p. 340). Threat assessments conveying worst-case scenarios are obviously detrimental to the risk management practice that emergency managers as well as policymakers must utilize since these assessments depict attackers with the full extent of weapons that can possibly be possessed coupled with conducting operations error-free against a target of known and limited capabilities.

Absent data that informs of attacker capabilities, analysts producing threat assessments must rely on other known or potentially relevant factors that can reduce the arrival at a worst-case scenario assessment. Unfortunately, it is difficult to attribute cyber attacks to a perpetrator which, in turn, makes it additionally complicated to reliably draw upon relevant factors or conditions in the geopolitical and technological space that can moderate a more accurate perception of attacker abilities (Lin, 2012). With the role that threat assessments play in understanding and quantifying the extent of threats to CI/KR from cyber attacks, emergency managers will be challenged to convey compelling information to private sector collaborators who must operate in a data-driven business model with heavy emphasis on return on investment (ROI).

Interestingly, early in their book, *Cyber Security and Cyberwar: What Everyone Needs to Know*, Singer and Friedman (2013) engage in discourse that attempts to temper perceptions of how severe the cyber terrorism threat against CI/KR truly is. They indicate that there have been no verifiable instances of individuals being injured or killed by cyber terrorism at the time their book was printed. One of the considerations offered is that massive cyber attacks are tough to execute upon in comparison to conventional physical terrorist attacks (Singer & Friedman, 2013). They further quote a professor from the US Naval Academy as having said "the threat of cyber terrorism, in particular, has been vastly overblown" (Singer & Friedman, 2013).

Additionally, Singer and Friedman (2013) indicate that the explosion of a dirty bomb or nuclear weapon would have a far greater impact from a terrorism perspective than would a cyber attack against a facility or particular CI sector.

What stands out most from Singer and Friedman's (2013) inclusion of this content in their text is that, in a later portion of their book, they very much draw upon conclusions and arguments advanced by Lin (2012) about the difficulties of threat assessments in cyber space. Their inclusion of this text could be seen as an attempt to provide a counter argument to the earlier one posed, but may also be interpreted as a means to call into question overall just what is truly known about the capabilities of any threat faced. Perhaps one point of clarification that should be noted in the way in which Singer and Friedman (2013) framed their earlier argument about moderating the concept of the cyber threat against CI/KR was that they did so under the premise of cyber terrorism enacted by terrorist organizations. While that threat certainly cannot be discounted, the more pertinent attacker, based on this literature review, appears to be nation states or nation state-sponsored actors. The Stuxnet worm's existence should support arguments that such capabilities exist and are being used today by nation states. This is perhaps where the most difficulty arises in developing accurate threat assessments—nation states have vast funds and resources available to them when compared to other malevolent actors. If the threat is truly viable, then worst-case threat analysis will be the likely trend when considering nation state actors until greater technological intelligence gathering can better inform what capabilities are actually possessed by such actors.

A final point to make about the threat assessment issue revolves around findings from research conducted by Jenelius, Westin, and Holmgren (2009). As discussed previously, allocation of finite resources by private and public sector entities for CI/KR resilience is

challenging at best. Utilization of worst-case analysis for threat assessments makes this practice cost prohibitive. Jenelius, Westin, and Holmgren (2009) determined that a perfect attacker scenario does not necessarily reflect a worst-case scenario. What this means is that an attacker with less than optimal intelligence and capabilities can potentially cause greater disutility against the target (Jenelius, Westin, & Holmgren, 2009). They also further determined that "spending more resources on an element is not necessarily better, since this may redirect the attack to more critical elements, causing the expected disutility for the overall system to rise" (Jenelius, Westin, & Holmgren, 2009, p. 25). In other words, threat assessments that cause potential targets to focus too intently on worst-case scenarios could result in a greater probability of success for attackers due to other exposures that may be overlooked as a consequence. Obviously, these findings coupled with the other cited research in this section of the literature review indicates improvement is still necessary in understanding the full nature of the cyber threat against CI/KR. Lin's (2012) conclusions on the potential threat appear most accurate based on the body of literature reviewed herein:

> "Given the overwhelming U.S. military advantages in traditional spaces of military competition, adversaries would be highly motivated to conduct asymmetric warfare against the United States in a conflict—warfare that takes advantage of specific U.S. vulnerabilities, such as those in cyberspace" (Lin, 2012, p. 347).

It is for this reason that emergency managers cannot ignore the cyber threat to CI/KR in the communities they serve and protect.

Legislation and Policy Challenges Hindering Optimal Resilience

Up to this point, the literature review has focused on the cyber threats to CI/KR and recognized challenges associated with quantifying those threats in a manner that best informs the

risk management process. The two previous sections of the literature review sought to address the first research question posed by the researcher: What cyber threats face CI/KR and how do those threats relate to the work of emergency managers? With the premise now being that the impetus exists for emergency managers to be familiar with and incorporate cyber security into their overall programs as well as understanding the challenges that lie ahead with quantifying the threats outside of worst-case scenarios, the literature review will pivot to cover legislative and policy issues that hinder optimal resilience. Previous sections pointed to existing legislation and policy that proved a governmental stake in protecting CI/KR. That section also sought to demonstrate why emergency managers should be aware of and understand the directives in both. This portion of the literature review will take a similar approach in looking at some of the applicable legislation and policies and explain why they introduce unknowns that hinder optimal CI/KR resilience to cyber attacks.

Based on the published body of literature researched for this content, aspects of the Fourth and Fifth Amendment in the United States Constitution are at the root of some of the most consistently referenced and discussed issues. Supporting case law, where applicable to further substantiate themes in the literature, will accompany the discourse on current problems hindering resilience. Emergency managers must be familiar with these issues in addition to the threat landscape in order to holistically work within the existing problem set framework as well as advocate for remediation in legislative and policy incongruences. As a preview to the complexity of the legislative and policy issues that follows, Singer and Friedman (2013) note that there were approximately 50 cybersecurity bills under review within both chambers of the United States Congress at the time of their book’s publication. That number alone indicates

heightened focus on the topic while unfortunately being compounded with challenges in passing appropriate legislation in the contemporary political landscape.

The Fourth Amendment to the United States Constitution states

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" (U.S. Const. amend. IV.).

The Fourth Amendment essentially prescribes limits as to the government's ability to conduct searches and seizures of individuals and property without a warrant specifying the details of either (Hunter, 2009). The authors of the Constitution obviously had then-present day experiences upon which to base the rights afforded in the Fourth Amendment. While the spirit of the Fourth Amendment continues in force, as the legal interpretations about the limits of the amendment have evolved, the case law in some rulings has introduced ambiguity in terms of how existing legal precedence either apply or do not apply to cyber space.

In the case of Boyd v. United States (1886), the U.S. Supreme Court ruled that the compulsory production of an individual's private papers violated the individual's Fourth Amendment rights. That alone would trend in line with the spirit of the Fourth Amendment's protections. However, in the case of Carroll v. United States (1925), the U.S. Supreme Court established precedence for a well delineated exception to the Fourth Amendment where it upheld the government's action in conducting a warrantless search of an automobile with probable cause. Subsequent case law has carved out more exceptions to protections afforded under the Fourth Amendment and thus introduced greater vagueness in the applicability of actions involving warrantless searches of non-physical systems.

The case of United States v. Ramsey (1977) is one such contemporary case that poses interesting considerations for monitoring and searching traffic on the Internet. This case addresses an instance of a customs and border protection agent opening envelopes of packages entering the country due to reasonable suspicion of narcotics being trafficked from the originating location. In this legal case, no warrant was possessed by officers conducting the inspections. The plaintiff sued alleging Fourth Amendment violations for the conducted searches. However, the Supreme Court held that searches of this nature are reasonable under the border exception to the Fourth Amendment (United States v. Ramsey, 1977).

An even more recent case, Doe v. Holder (2010), involved National Security Letters (NSLs) issued under authority from the USA PATRIOT Act (2001) to obtain records from Internet service providers without prior court approval or probable cause. Under the USA PATRIOT Act, recipients of NSLs are legally prohibited from disclosing they received an NSL. Fourth Amendment concerns abound from the original passage of the USA PATRIOT Act alone and this case obviously raises additional issues as to the warrantless monitoring enabled via legislation and case law precedence in the pursuit of preventing terrorism, which, under existing legal definitions, cyber attacks against CI/KR would qualify.

Deconstructing the implications for CI/KR as it relates to Fourth Amendment protections and existing case law precedents, Rice, Miller, and Shenoi (2011) offer some very thought provoking considerations around issues that either lack clarity or enable behaviors that will later be shown to be of concern to private sector entities that predominately own and manage CI/KR. “The nature of the critical infrastructure demands that cyberspace protection efforts be comprehensive to the extent possible” (Rice, Miller, & Shenoi, 2011, p. 3). Industries such as energy, financial services, and telecommunications currently undergo regulatory scrutiny from

the government via either government agencies or oversight entities (Rice, Miller, & Shenoi, 2011). However, the same regulatory structure for established sectors/industries only exists currently in a limited manner for cybersecurity (Rice, Miller, & Shenoi, 2011). If precedence exists for government monitoring in instances such as the activities conducted by the North American Aerospace Defense Command (NORAD) to protect against actions by other nation state militaries or intelligence services, one could argue that "substantive and comprehensive government monitoring of the cyberspace components of the critical infrastructure, similar to NORAD's monitoring of U.S. airspace" (Rice, Miller, & Shenoi, 2011, p. 4) is acceptable absent legislation stating otherwise.

Glick (2012) poses equally stimulating legal questions that remain untested in the courts regarding virtual inspections similar to those occurring at the physical border of the United States as originally addressed in United States v. Ramsey (1977). For instance, a decision rendered by the courts in United States v. Odland (1974) found that any

> "person or thing coming into the United States is subject to search by that fact alone, whether or not there is any suspicion of illegality directed toward the particular person or thing to be searched."

While virtual U.S. boundaries do not exist in cyber space, one could argue that communications originating from outside the U.S. and subsequently entering U.S.-based network infrastructure cross an international boundary that would subject them to similar governmental inspection as would be the case in the physical world (Glick, 2012). Recall that in the case of the United States v. Ramsey (1977), suspicion of contraband allowed a more rigorous search of a letter entering the United States. Under the existing cases noted above, precedence may exist for more detailed inspection of communications in a wholesale manner when crossing the functional equivalent of

an international border in cyber space—especially given the current state of highly malicious traffic constantly flowing across the Internet (Glick, 2012). While the actions can certainly be claimed as valid and necessary to protect CI/KR from malicious attack under the government's noted legislative powers (6 U.S.C. §§441-444, 2006; USA PATRIOT ACT, 2001; Homeland Security Act, 2002), it is easy to see how this practice can be problematic for private entities in the U.S. attempting to uphold privacy expectations of their customers.

Similarly, the Foreign Intelligence Surveillance Act (FISA), originally enacted in 1978, has caused consternation with protections provided under the Fourth Amendment. The Act was developed to ensure judicial oversight regarding the government's surveillance of individuals within the United States (Rice, Miller, & Shenoi, 2011). While initially more strict in its requirements for a court to allow approval of such surveillance, the USA PATRIOT Act significantly expanded the latitude of the government to monitor individuals within the United States when deemed of national security interest. Courts have subsequently held that the expansion of purpose criteria in conducting surveillance within the United States as amended by the USA PATRIOT Act did not violate protections under the Fourth Amendment (Rice, Miller, & Shenoi, 2011). With the national security implications of potential attacks against CI/KR, government surveillance may exceed tolerances deemed acceptable by the public at large and place private entities owning CI/KR in precarious positions.

Based on the current state of latitude afforded to the government via legislation, policy, and case law, Rice, Miller, and Shenoi (2011) find that "with the exception of physical searches inside the home, the Court is more likely to reduce, rather than preserve, Fourth Amendment Privacy protections" (p. 8). The applicability of the legislative discourse on the Fourth Amendment to the protection of CI/KR is rather straightforward in that the government has a

mandate to ensure the resilience and protection of CI/KR from malicious attacks in both the physical and non-physical spaces as a matter of national security. The threats, as covered in previous sections of the literature review, are verifiably real, which compels action commensurate to ensure security. However, since over 90 percent of CI/KR is owned by the private sector (Singer & Friedman, 2013), significant surveillance and privacy issues arise in relation to searches and seizures that should be protected under the Fourth Amendment of the U.S. Constitution. Obviously, such a situation fosters an environment that is less than ideal for public-private sector collaboration in pursuit of CI/KR resilience and must be addressed.

Shifting to the Fifth Amendment of the United States, the Amendment reads

> "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation" (U.S. Const. amend. V.)

While the majority of the Fifth Amendment does not apply to the topic at hand, the last clause, however, should be familiar to those who have studied emergency and disaster management law topics. Hunter (2009) provides several case law instances to address the pertinence of the Takings Clause in the Fifth Amendment to emergency management practitioners.

The United States Constitution contains a Commerce Clause that essentially gives the federal government regulatory powers (Rice, Miller, & Shenoi, 2011). These regulatory powers allow for oversight of practices by private entities such as establishing and measuring

compliance with standards, regulation of rates, and other functions deemed as serving to protect the public. Saxer (2005) discussed the origination of the clause as having been grounded in British tradition where property would be returned to the crown for public use when the benefit to many was greater than the benefit to an individual. The authors of the Constitution, however, wished to protect individual property owners' rights by preventing the government from abusing the power through indiscriminate taking. The qualifier of "just compensation" was included in the Takings Clause to ensure fair payment be made for any property taken under this authority. Contemporarily, this is often referred to as the concept of eminent domain, however that is only one of two forms of taking under the lause (Rice, Miller, & Shenoi, 2011).

Traditional use of eminent domain by the government has required the taking to be for public use (Saxer, 2005; Rice, Miller, & Shenoi, 2011). The lesser-known form of taking occurs through the government's ability to regulate private property. In this case, the regulation may be so intrusive to the private entity that the property owner sues the government to establish a regulatory taking and receive just compensation (Rice, Miller, & Shenoi, 2011). While the just compensation criterion attempts to protect private owners from abuses of takings, both Saxer (2005) and Kochan (1998) indicate the relaxation of requirements around the public use standard for the Takings Clause has subsequently weakened the protections originally intended within the Fifth Amendment.

Where the Takings Clause becomes particularly salient for the protection of CI/KR is in how it has evolved in recent years through executive acts. In 2006, then President George W. Bush issued Executive Order 13406 clearly stating that the United States is responsible for protecting the rights afforded to private property owners (Rice, Miller, & Shenoi, 2011). However, several exemptions to the order accompanied the policy including taking property to

meet “military, law enforcement, public safety, public transportation or public health emergencies” (Rice, Miller, & Shenoi, 2011, p. 7). Again, Hunter (2009) offers cases for emergency managers to consider in which public safety or public health emergencies served as the impetus for the federal government temporarily taking private property. It is reasonable under the heightened homeland security mindset to conclude that attacks on privately owned critical infrastructure and key resources would constitute a public safety, law enforcement, military, public health, or public transportation emergency and the exemption under Executive Order 13406 allowing for the taking of that property would be invoked. While the private property owner could certainly seek legal remediation in a court of law to test the legality of the executive order, the timeliness of any such hearing and ruling, especially considering likely appeals, would draw out for some time—perhaps long after the emergency that precipitated the taking had passed.

Beyond the Fourth and Fifth Amendment issues summarized in the previous paragraphs, other challenges exist within the legal and policy landscape that continue to hinder achievement of improved resilience against cyber attacks for CI/KR. While the Department of Homeland Security has been designated as the agency on point for cybersecurity at the federal level, numerous other federal agencies have significant roles that in some cases add ambiguity to lines of authority (Young, 2012).

For instance, the USA PATRIOT Act orders the United States Secret Service to establish an Electronic Crimes Task Force “in order to prevent, detect, mitigate, and investigate attacks on the U.S. financial systems and critical infrastructure” (Young, 2012, p. 292). Questions around implications for cyber warfare and the Department of Defense’s role providing the nation’s military force remain unclarified in the national policy discourse (Young, 2012). The NSA

provides significant signals intelligence and may have the ability to see a threat coming through its routine work. However, it has no authority, though arguably is very capable, to take preventative action (Young, 2012). The Federal Bureau of Investigation possesses the legal authority to investigate criminal acts in cyber space for the United States, which requires a close synergy between that agency, the broader Department of Justice, and the Department of Homeland Security. While "no federal organization helps protect commercial networks" (Young, 2012) as a practice, the preceding investigation of ambiguities or challenges around the Fourth and Fifth Amendment in this regard as well as the interpreted intent of 6 U.S.C. §§441-444 (2006) indicate both a vested interest by the federal government in protecting CI/KR that is predominately privately owned as well as highlight other legislation and policy that would seem to imply federal organizations are expected to assist in the protection of commercial networks.

Perhaps one of the most complicated topics due to the relatively untested methods of recourse up to this point in both practice and case law centers around methods of response to cyber attacks against CI/KR. As Vasilescu (2012) points out, in traditional war tactics, the nation being attacked has the right to defend itself militarily. However, it is unclear if an attack targeting cyber space warrants response with military action or what the escalation of force progression should be (Vasilescu, 2012). Attribution of an attack alone is difficult at best (Zhang, 2011). While physical damage can be assessed and response in kind can occur, determining the extent of damage in a cyber attack is difficult unless the results also manifest in physical damages and/or casualties. Lacking an accurate assessment of damage, it is difficult to determine what a commensurate response in defense of the damage incurred truly is.

Furthermore, as Young (2012) noted, federal organizations do not help protect commercial networks by practice. If a nation state or nation state sponsored attack against CI/KR

in the United States results in either physical or non-physical damages, private entities currently do not have clarity on what actions they can take to defend their infrastructure—especially from a response in kind perspective. Indeed, response actions to cyber incidents could constitute violations of domestic and international laws (Zhang, 2011). Research indicates that "private industry may be more likely to use an active defense than sovereign states" and this means that "a private company action can be mistakenly interpreted as hostile activity from the U.S. government" (Zhang, 2011). Certainly, the threats against CI/KR warrant resilience and defensive actions, but it appears that the legislative and policy landscape is relatively immature to establish boundaries and direct actions in both the public sector and the private sector.

Literature Review Summary

The preceding literature review serves several purposes in supporting arguments posed within the scope of this thesis. First, articulation of the pertinent legislation and policy substantiates a significant federal stake in the authority to regulate and duty to recognize and protect assets, capabilities, and systems classified as critical infrastructure or key resources in the United States. Emergency management practitioners and academics alike should be very familiar if not well versed in these legislative and policy items since many of them form the bedrock of contemporary emergency management and homeland security responsibilities. It is because of the inherent applicability of these statutes, acts, and policy mandates to the emergency management discipline that practitioners and academics must understand the cybersecurity concepts incorporated in said policy and legislation. Choosing to address only physical threats that are either natural or human-made ignores this very valid and pertinent topic and fails to embrace the all-hazards premise that is core to the emergency management profession.

Published literature affirms that there is current immaturity in the ability to clearly articulate the capabilities possessed by potential malevolent entities seeking to disrupt CI/KR in the United States either domestically or abroad. The fact that nation states have emerged as potential actors in CI/KR attacks only underscores the complexity of rendering accurate threat assessments upon which to base legislation, policy, and subsequent protective actions aimed at increasing resilience and reducing the impact of any completed disruption. What this truly signals is that cybersecurity in general is a rapidly evolving topic and there is comparatively limited peer-officiated literature on the subject as well as actual instances of known successful CI/KR attacks. Emergency managers will most certainly be challenged to keep pace with the dynamic nature of the issue in conjunction with their ever-expanding roles in protecting the communities they serve.

Admittedly, it is understandable though nonetheless an apparent issue throughout the literature review that the constantly evolving threat landscape has resulted in the inability for legislation and policy to maintain commensurate pace. As Singer and Friedman (2013) noted, over 50 cybersecurity acts were in various stages of review in both chambers of Congress last year alone. The future legislative and policy landscape only looks to become more complicated through heightened regulatory scrutiny and increased connectivity of CI/KR to the Internet itself. Threat assessments based on worst-case scenarios due to the lack of verifiable data will likely compound the level of attempted regulation through legislation and policy that the federal government has the authority to develop under already existing incongruent acts and statutes. Emergency managers must become a voice in the greater efforts to reconcile these gaps or conflicting mandates and act as a conduit between the public and private sector to foster greater resilience of CI/KR. This will require working across levels of government and sectors—actions

both very much already a part of an effective emergency manager's existing responsibilities for other threats in their communities.

This literature review also highlighted some gaps that the thesis seeks to address in subsequent sections. Practically none of the literature except for the very recent course description from American Public University argues the issue of cybersecurity for CI/KR is a topic salient for emergency managers. Though cybersecurity for CI/KR itself is recognized and discussed in detail in several of the cited publications herein, few if any addressed stakeholders at the local or state levels in any form of public sector agencies. Yet, the nature of the threat and the ongoing need to address protection and resilience practices seem to rather overtly align with responsibilities that emergency managers already have in their roles either by legislation and policy or through historical practices foundational to the emergency management discipline itself.

Another gap in the existing literature that this thesis attempts to address is the reconciliation of the various policy and legislative issues applicable to the protection and resilience of CI/KR and how emergency managers can best set about effectuating awareness and change. While some authors offer recommendations in the federal space to improve the situation, those recommendations rarely identified responsible parties or those roles well-suited to collaborate on improvements. Later sections in the thesis will demonstrate the importance of emergency manager action to influence improvements, build synergy where it continues to flounder between the private and public sectors, and leverage acquired cybersecurity knowledge to develop informed and holistic emergency plans and response protocols.

Research Methodology and Procedures

Creswell (2009) has developed a seminal work on research design that is recognized throughout the academic community at the undergraduate, graduate, and terminal levels. The text, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, served as an authoritative guide in framing the research approach used within this thesis. Based on assessment of the three research methodologies prescribed within the Creswell (2009) text, the researcher determined that a qualitative research methodology and its supporting components afforded the best mechanisms by which to view the issue, conduct the necessary supporting analysis, and articulate the findings and recommendations.

"Qualitative research is a means for exploring and understanding the meaning individuals or groups ascribe to a social or human problem" (Creswell, 2009, p. 4). The research questions developed in the early stages of investigating the topic reflect the underlying concept of the qualitative research methodology—one of emergent questions and techniques. Recognizing the inductive nature of the topic, the researcher sought to focus on the individual meaning applied to the issues as suggested by Creswell (2009) regarding CI/KR resilience against cyber threats. As Locke, Spirduso, and Silverman (1987) note, qualitative research is the ideal methodology to cognize social phenomenon on issues requiring an investigative approach requiring inductive interpretation. Such interpretation relies on acknowledged methods that include comparing and contrasting as well as classification and duplication among other formal rigorous and recognized procedures (Miles & Huberman, 1984). According to Creswell (2009), these procedures are hallmarks of the qualitative research design methodology and provided a functional framework through which the researcher could depict the complexity of the issues.

The researcher approached the thesis with dual worldviews that supported the qualitative research methodology employed. The advocacy and participatory worldview is based on the

belief that research investigation must be coupled with politics and political agendas (Creswell, 2009). This worldview essentially reflects the researcher's intention to advance an agenda that seeks to reform issues experienced by individuals or institutions including, potentially, the researcher's life experiences as well (Creswell, 2009). An advocacy and participatory worldview gives a voice to the individuals or institutions intended to benefit from the advocated agenda and further supports a means for researchers to conduct research salient to impactful issues in their own lives. Since much of this thesis addresses legislative and policy challenges that affect the public and private sector dynamic in achieving resilient CI/KR, it is rather straightforward to connect the relationship in legislation and policy to the mechanism through which both come into existence: politics. As such, the researcher sought to qualitatively advocate for changes that will improve the work emergency managers must do and ultimately the safety of the communities in which they serve.

In addition to the advocacy and participatory worldview, the researcher also used a pragmatic worldview in developing the thesis topic and conducting the commensurate research. Pragmatism "arises out of actions, situations, and consequences rather than antecedent conditions" (Creswell, 2009, p. 10). This worldview afforded the researcher with latitude in choosing strategies of inquiry most effective for the topic. Additionally, reflective of the pragmatic worldview according to Creswell (2009), the researcher recognized that the issue under inquiry was not constrained to a singular context; rather, it contained historical aspects from an issue evolution perspective as well as political factors in the development and maturation of legislation and policy and social influences for the public-private sector dynamic.

Role of the Researcher

Any research endeavor involving the advocacy and participatory worldview has the potential to touch upon a topic directly impacting the researcher in some way. The role of the researcher within the scope of this thesis was to address a relatively emerging issue that involved interests of the researcher while accompanied by a solidly executed research methodology that supported advocacy for identified areas of improvement. To that end, the researcher's background was an important consideration in the selected methodology and the accompanying procedures.

From a professional experience perspective, the researcher has worked with information technology computing resources to varying degrees for 25 years. The past 14 years have consisted of information security responsibilities spanning the application and infrastructure layers of the technology stack. The researcher holds a Bachelor of Science degree in Computer Science and also possesses a Certified Information Systems Security Professional (CISSP) designation from the International Information System Security Certification Consortium. Additionally, the researcher has worked as an emergency management practitioner for nine years for a municipal government agency at the county level, has completed several Federal Emergency Management Agency (FEMA) certifications, and is a Master of Arts degree candidate in Emergency and Disaster Management.

The aforementioned credentials and experiences led to the identification of a topic that potentially substantiated validity in the convergence of cybersecurity with the emergency management discipline in the protection of CI/KR. The questions noted in the problem statement section of this thesis formed the basis of inquiry guiding the researcher's investigation into the merits of the topic and the value further research on the issue could bring to advancing the body of knowledge in the emergency management discipline. However, due to the researcher's

background and credentials, concerns of potential researcher bias inadvertently influencing the research findings warranted heightened diligence in the research method and supporting methods of inquiry. Failures in conducting rigorous research reflective of academically acceptable standards calls the validity of the analysis and conclusions into question and fails to advance an important topic within the emergency management discipline.

Data Collection Procedures

The researcher used several information sources to locate and compile pertinent content for the literature review and analysis sections of this thesis. Aligning with Creswell's (2009) description of the qualitative research methodology, the researcher relied on textual and image analysis and formal methods to identify themes and interpret patterns contained within the sourced content on the topic. Following practices established in the academic community, the researcher first conducted a comprehensive search in online library repositories for pertinent peer reviewed academic journal articles addressing one or several aspects of the thesis topic. Keyword search terms ranged from broad concepts such as "cybersecurity," "critical infrastructure," and "security legislation" to more specific keyword searches including variations on "emergency management cybersecurity," "critical infrastructure laws," "constitutional issues with critical infrastructure protection," and "public private sector collaboration in cybersecurity." EBSCO, LexisNexis, and JSTOR returned much of the peer reviewed content in terms of academic journal publications. While the researcher tended to observe search results for publications in the past five years as being most prominent, older articles were included in the body of research initially analyzed since articles published beyond five years ago could offer potentially useful insights into issues at the time that remain just as salient as current-day publications.

While peer refereed academic journals are generally considered the most rigorously vetted sources for scholarly research, numerous textbooks throughout the Master's Degree curriculum have afforded a very insightful look into contemporary emergency management issues affecting the discipline. Therefore, the researcher leveraged textbook content on emergency and disaster management or books published by notable scholars in the field of cybersecurity and infrastructure protection to further diversify the sources upon which the literature review and subsequent research analysis occurred. Texts that related to the topic ranged from being those generally addressing emergency and disaster management concepts to those that touched upon policy and politics as well as specific CI/KR cybersecurity problems.

Since much of the thesis is predicated on the idea that federal legislation and policy for cybersecurity resilience for CI/KR is incongruent and thus resulting in suboptimal resilience conditions, the researcher conducted significant investigation into applicable policy and legislation enacted by the legislative and/or executive branches as well as case law rulings rendered by the judicial branch. This content, though not of academic origins, remains substantially credible for the purposes of the research conducted herein since the laws, policies, and court rulings form a well-documented framework upon which much of the research topic is based or influenced. In most instances, the researcher sought supporting publications in either academic journal form or textbook form as a mechanism to validate theories about the role specific legislation and/or policy as well as case law had as factors affecting the clarity or ambiguity surrounding efforts to holistically protect CI/KR from cyber attacks.

Lastly, the researcher looked outside formal academic, textbook, and legal sources to identify other content germane to the research topic. This included seeking magazine publications, speeches, or other public discourse from credible industry sources that could

augment support for identified themes and patterns from the more rigorous publications comprising the majority of the body of knowledge sourced for the thesis research. Content developed by governmental officials, cybersecurity industry experts, and recognized periodical publishers received the most attention from the researcher. These were preferred sources rather than sources generally subject to a high degree of individual opinion such as editorials in historically controversial media or informal online publications with typically relatively limited audiences that scrutinize the content.

Over 60 sources comprised the initial body of research conducted to assess the topic and its merits. Sources addressing the mechanics of academic research methodologies also encompassed the content reviewed by the researcher throughout the information gathering, literature review, research methods, and analysis portions of the thesis. In many cases, initial sources under review pointed to other publications, legislation, or case law that also became part of the complete body of knowledge leveraged by the researcher throughout the development of the thesis content. Sources that appeared to offer conflicting findings remained as part of the overall body of research. In those cases, themes or patterns that contrasted with others identified were tracked through textual analysis procedures. This ensured that researcher bias did not result in the possible disregard of potential counterpoints that challenged the research questions or conclusions drawn through the analysis conducted.

Data Recording Procedures

Initial data recording procedures involved very basic practices often employed by researchers when first acclimating with qualitative data. Saldaña (2013) indicates this typically consists of manual highlighting and note taking and the researcher employed both techniques as a first pass in becoming familiar with the data corpus. Such techniques can also qualify as pre-

coding where, while admittedly unrefined, the researcher begins to identify potential themes and patterns that surface in the body of literature under review (Saldaña, 2013). In essence, this practice also begins the process of identifying what Auerbach and Silverstein (2003) refer to as "relevant text" where the researcher distinguishes content that appears applicable from other text that may be superfluous to the research.

Data Analysis Procedures

Much of the analysis in this thesis is derived from a qualitative technique referred to as coding.

> "Coding is a heuristic (from the Greek, meaning to "discover")—an exploratory problem-solving technique without specific formulas to follow. Coding is only the initial step toward an even more rigorous and evocative analysis and interpretation for a report. Coding is not just labeling, it is *linking*: 'It leads you from the data to the idea, from the idea to all the data pertaining to that idea'" (Saldaña, 2013, p. 8).

The researcher followed the coding approaches discussed by Saldaña (2013) in the course of compiling the data corpus for analysis. Saldaña (2013) advises that detailed explanations of coding approaches should not be included in formal research papers as it is a rather behind-the-scenes activity, so brevity in specifics will be maintained herein.

Given the body of literature under review for the thesis, the author sought the use of Computer Assisted Qualitative Data Analysis Software (CAQDAS) to arrange and link codes in a manageable fashion. After initial highlighting and notations, the researcher loaded the data corpus into the Atlas.ti 7 qualitative data analysis software and leveraged both manual and auto coding capabilities to code the relevant data and link it to ideas persistent across the reviewed literature. Several passes to refine codes and establish coding categories in-line with

recommendations by Saldaña (2013) also occurred before any formal analysis was conducted. Upon completion of coding activities, the researcher reviewed a software-generated network view of the concept linkages in the CAQDAS software to guide the development of the qualitative narrative that follows in the subsequent section of this thesis.

Analysis and Recommendations

From the literature reviewed throughout this thesis, it is clear that the federal government maintains a significant stake in the protection of critical infrastructure and key resources from threats that could result in catastrophic outcomes for the homeland. Evidence to support the federal government's authority and responsibility to ensure the protection of critical infrastructure exists in the myriad of legislation and supporting policies within the United States Code, various legislative acts, directive policies, and subsequent case law—both those discussed within the context of the literature review as well as others not addressed herein. In its protectionism role, governments must take steps that would deter harm from coming to its citizens, the homeland, its ability to operate, and the country's foundational ways of life. In essence, the federal government must seek to uphold the rights and structures enumerated in the United States Constitution. Determining the best course of action through which to achieve this significant responsibility can be difficult at best given the complexity of all that must occur under this broad charge.

Recall that Singer and Friedman (2013) as well as Rice, Miller, and Shenoi (2011) state that the vast majority of the CI/KR in the United States is owned by the private sector. Arguably, the protection of CI/KR therefore rests not in the hands of the government, but in the private sector owners of these systems and assets. Therefore, governments cannot singularly achieve the necessary security and resilience of these critical systems without a strong synergy amongst the

private sector owners of the infrastructures themselves. Kelly and Hunker (2012) echo this same point and acknowledge that "there is a divergence between cyber security responsibility, because the government must protect the nation from crippling attacks, and cybersecurity control, because the government does not manage the assets or provide the function that must be protected" (p. 233).

This research sought to not only offer a compelling argument for emergency managers to understand the importance of cybersecurity as a component of their plans, but to inform the practitioner community of the challenges that comprise the landscape of the issue itself. The researcher identified not only recurring themes through qualitative analysis that supported the argument of importance and applicability to emergency managers, but themes that also signaled issues in the public-private sector dynamic tied to legislative and policy factors that have failed to capitalize on a productive, collaborative relationship between both sectors. The absence of a requisite synergy is a theme that emerged in literature by Singer and Friedman (2013), Zhang (2011), MacCarthy (2012), and Kelly and Hunker (2012). Such a lack of effective collaboration between the public and private sector points to a significant impediment in meeting the legislative and policy mandates enacted at the federal level of government.

If the premise that ineffective relationships are hindering optimal resilience of CI/KR against cyber attacks is valid as appears supported by the literature, understanding and addressing the causative factors is important for informing actions aimed at improving the current state. Another theme surfaced during the qualitative analysis of the data corpus that indicates a lack of trust, especially harbored within the private sector, heavily affects the public-private sector dynamic. This lack of trust stems from several factors which, on their own, appear

to hinder collaboration for optimal resilience while, in the aggregate, create a substantial impediment that potentially requires several actions in tandem to alleviate.

One problematic area affecting trust in the private sector stems from the government's regulatory authorities. As discussed in the literature review, the government possesses a substantial ability to regulate aspects of the private sector through the Commerce Clause in the Constitution (Rice, Miller, & Shenoi, 2011). While heavy regulation is not new to some sectors such as energy or the defense industrial base, others such as the financial services sector, healthcare and public health, and information technology are finding themselves subject to heightened scrutiny and directive actions from the federal government (MacCarthy, 2012). Although some sectors may be accustomed to a constant regulatory presence and influence on their work, that does not necessarily mean that it fosters a productive relationship. As Comey (2014) alluded to in his address at the 2014 RSA Conference, regulation that is perceived to be overbearing or only beneficial to one side—in this case the public sector—can result in a grudgingly cooperative relationship in which the private sector does only what it is compelled to do. Admittedly, this conclusion cannot be said to be applicable in all cases. However, as Kelly and Hunker (2012) state, "In the U.S., there is strong resistance to any form of direct government regulation of any aspect of cyber space" (p. 215) and "it is more common that government has policy goals that it simply does not have the capabilities to achieve" (p. 227).

Adding to the frustrations the private sector harbors around trust in collaborating with the government is the secretive way in which the federal government compels private sector organizations to share information about customers/clients through National Security Letters (NSLs). Recall from Rice, Miller, and Shenoi (2011) that privacy issues permeate much of the current discourse regarding the government's involvement in national security. NSLs take

something very important to the private sector, information about their customers, and place it in the hands of the government while preventing the private sector from being able to notify the impacted customers that their information was handed over (Rice, Miller, & Shenoi, 2011). When customers trust their information to a private entity, there is often the expectation that it is protected. Giving that information up is seen by the private sector as a violation of that trust and a potential harm to brand reputation. Again, Kelly and Hunker (2012) acknowledge that the public may take issue with the government intruding in what transpires with private sectors regarding cyber space and this places the private sector in the middle of both governmental and customer expectations with consequences on either side.

The qualitative analysis of the data corpus for this thesis also indicates that information sharing across the public and private sector is insufficient to achieve the desired levels of CI/KR resilience against cyber attacks. As evidenced in previous findings noted herein, the federal government possesses legal authority to compel compliance in meeting the mandates of applicable legislation and policy. Besides regulation (which can involve intensive auditing), the government can seek information from private sector entities about threats, policies, practices, breaches, and other topics germane to the information security posture of an entity. However, this information sharing is often derided by the private sector since it tends to be a one-way sharing relationship. Rosenzweig (2010) remarks that the Information Sharing and Analysis Centers (ISACs) have "produced little more than the repetitive refrain that government can't share intelligence with the private sector and the private sector sees little to gain by sharing with the government" (p. 266). The rationale noted for why the government tends to not share information with the private sector is due to information often being classified (Rosenzweig, 2010). Comey (2014) echoed this issue in his RSA remarks by acknowledging that the

government must do a better job of sharing threat intelligence and other pertinent information with the private sector and it must commit to issuing security clearances where appropriate to enable that information sharing. Further, the private sectors see little incentive to share information because of this one-way sharing model and due to the increased regulatory oversight that could be imposed upon them when sharing information in good faith. The Constitutional precedence under the Takings Clause compounds this reluctance from the private sector to altruistically partner in protection activities with the government.

During the literature analysis, it became apparent as well that the private sector's avenues of recourse for deterrence, especially when attacks originate from international sources or those involving nation states, is ambiguous at best. Consider a private sector entity's CI/KR is subject to a cyber attack. Certain actions that the entity may choose to take as a means to deter the attack "may violate domestic and international laws" (Zhang, 2011). Vasilescu (2012) remarks that in the case of traditional war actions, the victim state has an acknowledged right to defend itself with military measures. However, the response is not so clear in cyber space as to whether conventional weapons or defensive mechanisms should be involved. "How should a private electric company react if its grid appears to be subject to infiltration from an unidentified Chinese source? Is it disabled from taking action by the potential that the foreign source might be operating at the direction of Chinese authorities" (Rosenzweig, 2010, p. 261)? Such an unresolved issue further strains public-private sector relationships when the private sector may not see any protective avenues afforded by the federal government (Rosenzweig, 2010).

As Singer and Friedman (2013) noted, the end of 2013 saw over 50 pending cybersecurity laws in various stages of review within Congress. The enactment of Presidential Policy Directive 21 demonstrates a very recent attempt by the Executive branch to mandate

policy within this space as well. Overall, a consistent theme that emerged from much of the literature indicates the belief by the government that significant additional legislation and policy can improve the issue of resilience for CI/KR and cybersecurity overall. Yet, as another identified theme throughout the literature indicates, the level of incongruence and unresolved implications of case law rulings would support an argument that legislation and policy are not panaceas for the issue.

Recommendations

The intent of this portion of the thesis is to address recommendations for emergency managers regarding CI/KR resilience against cyber attacks. The researcher has developed recommendations based on analysis of the most salient issues affecting emergency managers at the local and state levels. This includes how best to understand the topic, navigate the various issues, and advocate for change where it is within their abilities to do so. The aggregate outcome is intended to help emergency managers achieve improved CI/KR resilience in their communities.

As rewarding as it would be to posit recommendations addressing the full landscape of issues affecting the legal and collaborative dynamics on CI/KR resilience, such an endeavor is beyond the scope of this thesis. Recalling that this thesis sought to identify why the issue is important to emergency managers and what types of challenges awaited emergency managers as they worked to include cybersecurity of CI/KR into their mitigation, preparedness, response, and recovery activities, it rather makes sense to elucidate the factors that dominate the issue at the present. While it would be detrimental to emergency manager efforts at achieving greater CI/KR resilience against cyber attacks to lack a familiarity with the broader issues, several of the challenges clearly require contributions by the private sector as well as specific improvements in

the federal government that local and state emergency managers may be unable to fully effectuate.

First and foremost, local and state emergency managers must come to understand the applicability of this evolving topic within the practitioner and academic community through intentional and engaged learning and discourse. Several avenues for achieving this can exist though admittedly few are readily tailored for emergency managers at this time. One directly applicable offering, as noted within the Literature Review, is the American Public University System's recent creation of a Master's Degree course covering perspectives on cybersecurity for emergency managers. This course appears to address the topic and relate it in a way that is most impactful for those formally studying emergency management in an academic setting. Course evaluations will undoubtedly serve to verify the value of this educational offering, but it may be a very successful course upon which other universities can model their inclusion of the topic within their established curriculums. Courses on the subject should not remain limited to the Master's Degree level either—undergraduate and terminal degree programs in addition to university certificate programs should consider expanding their offerings as well to include the topic.

While university courses are one avenue for increasing understanding and discourse on the topic within the emergency management practitioner community, many current position incumbents lack the ability to enroll in university courses. Other training sources such as the Emergency Management Institute (EMI), the International Association of Emergency Managers (IAEM) Conference, and the National Association of Emergency Managers (NAEM) Conference, as well as state and local emergency management conferences can provide training and avenues for discourse as well. There is a greater likelihood of visibility for this topic through

those organizations than through academic courses since the majority of current practitioners are likely not pursuing formal education through the university setting. State emergency management agencies may be ideally poised to socialize and advance training on the topic since they are vital to bridging the relationship between the federal level and local practitioners. The topic appears to have decent visibility at the federal level (albeit it is notably disjointed as evidenced in the legislation and policy realm), but the Literature Review and qualitative analysis did not support the same level of visibility at lower levels of government.

Training on the applicability of cybersecurity for CI/KR in the emergency management discipline must also consist of information about the existing public and private sector dynamic hurdles that challenge the attainment of greater resilience. Lacking this knowledge would place emergency managers at a disadvantage in enabling them to navigate the topic most effectively in their efforts to improve the current state. Such information should, at a reasonable level, provide insights into the current legislative and policy incongruences that are straining public/private sector relationships and require reconciliation. As this can become a rather complex aspect of the topic to convey, training content developers should strive to achieve a balance based on the nature of the offering. Academic courses have the luxury of delving more deeply into complex topics and can thus elaborate on the legislative and policy dilemma far better than conference or online/in-residence EMI courses may be able to achieve. Nonetheless, failing to address the legislative and policy factors, as demonstrated in this thesis, would be severely ignoring a considerably influential problem within the overall topic landscape. It may be best for representative organizations and academic institutions to jointly develop outlines or course goals to consistently achieve the desired level of awareness and education among the practitioner community.

Outside of structured training, emergency managers can seek information on the cybersecurity threat to CI/KR from periodicals, peer-reviewed journals, news outlets, and their own colleagues. Again, organizations such as the IAEM, NAEM, or EMI can be influential in this regard by developing reading lists or centralized sources of reference materials to which emergency managers can refer on a regular basis. The literature review in this thesis supports the fact that rigorous research is underway on this subject and publications such as *Emergency Management Magazine* have addressed facets of the topic as well in recent issues. As emergency managers hone their crafts and further refine the discipline, they have become accustomed to frequently incorporating new knowledge into their practices and professional endeavors. The value of a self-initiated informal learning approach should not be underestimated in this case. State levels of government are poised to disseminate information pertinent to the subject as well to local emergency managers since many state emergency management agencies serve as information clearing houses for their local counterparts.

Acknowledging the importance of the topic by emergency managers and seeking education on the issues is one set of recommendations to address the issues discussed herein. As should be evident though, the public sector cannot achieve the strides necessary to effectuate greater CI/KR resilience against cyber attacks alone. A strong synergy must exist between the two sectors and local emergency managers will likely be the catalysts in building and maintaining these critical relationships. Such relationships are not only necessary from an ownership and management of CI/KR perspective—the private sector enjoys significantly greater access to information security professionals that work in the protection space than local or even state emergency managers can mobilize on their own. While it is unreasonable to expect emergency managers to become experts in the highly technical nuances of information security,

it is quite feasible to establish partnerships with the private sector that leverage their information security experts' knowledge, skills, and abilities in a mutual attempt to protect CI/KR. Such a relationship can be quite advantageous for the private sector from a risk management standpoint provided that emergency managers can successfully overcome the factors hindering collaboration.

Successful emergency managers excel at relationship building—it is foundational to their ability to bring individuals and groups together in planning or during an emergency. Building and maintaining relationships with the diverse and often changing points of contact that emergency managers have is certainly challenging even for the skilled practitioner. This research has highlighted an emerging area of focus for emergency managers that will require them to apply their relationship building skills yet again with those in the private sector. As discussed, resilience for CI/KR requires a significant commitment from private entities that own and manage the assets and infrastructure. Emergency managers must draw from their knowledge, skills, and abilities to bridge the previously discussed public-private sector dynamic issues if resilience is to make marked improvements. MacCarthy (2012) and Kelly and Hunker (2012) emphasize the importance of collaborative groups and the need to grow that approach further in this realm.

At the local level, emergency managers have likely worked with private sectors in preparedness and potentially response efforts for other emergencies or disasters that apply to private entities in the community. Emergency managers should consider how their existing hazard and vulnerability analyses (HVAs) may need to incorporate the cybersecurity threat to CI/KR in their communities and then revisit the subject with their private sector counterparts. Emergency managers who come to the table with training offerings, abilities to share pertinent

information with their private sector collaborators, incorporation of cyber attack scenarios in tabletop or actual exercises, and providing access to conferences or other networking events that will foster greater knowledge and partnership are more likely to experience success in their efforts. If formal collaborative groups involving both public and private sector representation at the local level do not exist, emergency managers are ideal candidates for advocating for the creation of such groups. The researcher's own county has a disaster council comprised of public, private, and non-profit entities in the community ranging from the biggest employers, hospitals, and universities to smaller churches, the American Red Cross, and other volunteer organizations. Such councils offer an ideal mechanism through which to raise and address the topic of CI/KR resilience against cyber attacks with pertinent private sector entities.

State emergency management organizations can also be very influential in improving the public-private sector dynamic to facilitate greater CI/KR resilience against cyber attacks. When it comes to larger organizations with a presence in multiple communities throughout a given state such as energy, financial services, and telecommunications, state emergency management agencies are in a position to work across local jurisdictions with corporate or regional offices to raise awareness and open lines of communication for emergency managers. State emergency management agencies can also enable visibility for the topic through its inclusion in hosted conferences, statewide messaging in programs or press releases, and via formation of partnership organizations intended to bring various stakeholders to the table. Where emergency managers at the local level may struggle with bridging the public-private sector partnership to address this topic, state emergency managers can potentially assist.

One very prominent theme in this research affirmed the disconnect that exists in legislation and policy surrounding cybersecurity resilience for CI/KR. Emergency managers are

in most cases, not legislators. However, they may often find themselves working with legislators and forming professional relationships that affords them the opportunity to provide candid and trusted feedback into legislative activities from a non-political perspective. While local emergency managers can certainly build these relationships with their city councils and county boards, this research has identified many of the problems existing at the federal level. It is therefore important for emergency managers at all levels to leverage their collective voices through established representative entities such as the NAEM or IAEM as well as via state-level legislative representatives in the House and Senate. Providing feedback on concerns raised by private sector entities and collaborating on legislative and policy developments can incorporate measures to address and ameliorate those concerns.

As Singer and Friedman (2013) indirectly alluded to in their text, legislation should not be looked to as the single lever pulled on to address the problems affecting the achievement of optimal CI/KR resilience against cyber attacks. It is naïve to believe that relationships and advocacy alone can resolve the legislative challenges facing this topic. Some of the most foundational tenets of the U.S. Constitution such as privacy, search and seizure, and takings reflect the natural evolution of our nation's growing understanding of an emerging issue. Time and continued reliance on the checks and balances built into the governmental structure of the United States must be recognized as factors influencing this topic. That being noted, the governmental structure provides avenues in various places for direct action and inclusion of ideas and practices for codification into law. Thus, effective navigation of the legislative and policy landscape by emergency managers and others with a viable stake in this issue must occur in tandem to the governmental machinations themselves.

The concept of the Information Sharing and Analysis Centers for the various sectors showed promise in their early inception. MacCarthy (2012) points to the groups themselves being variable in their actual successes in bridging the public-private sector gaps such as those addressed within the scope of this thesis. There are clearly some success in sectors such as the Financial Services ISAC, which was recognized in 2013 at the RSA Conference for its contributions to information sharing regarding cyber threats and cybersecurity. Recent formation of a Retail Services ISAC following the massive data breach with Target appears to substantiate the need for such groups even further. Emergency managers should investigate the most effective way to work with these organizations as one way to improve the relationships and bring the private sector along in their efforts to address mitigation, preparedness, response, and recovery activities for their communities.

Future research has the opportunity to investigate and measure the effectiveness of the ISAC concepts and provide recommendations for practices that successful ISACs can share with less effective ones. Research efforts should also address training and knowledge sharing within the emergency management and academic communities about cybersecurity for CI/KR since it was determined within this thesis that the emergency management community still lacks a solid understanding of the topic. An additional area of focus for future research could be on whether all sectors face the threat equally or if certain sectors are at greater risk for cyber attacks. Finally, the researcher found little information about the application of cyber risk management to risk management practices leveraged in the homeland security and emergency management physical realms. Information technology risk management methodologies are rather robust and are numerous in quantity. Likewise, several risk management methodologies currently exist outside of information technology. It is not clear whether either sets of methodologies consistently align

with each other, yet it is important to investigate this aspect since emergency management derives much of its mitigation and preparedness fundamentals from risk management concepts.

Conclusion

Cybersecurity for critical infrastructure and key resources has gained heightened visibility in recent years due to the growing capabilities of malevolent actors around the world. Much of the United States' stability and safety rests on the resilience of these systems and assets that predominately lie in the hands of the private sector. The government possesses legal responsibilities to ensure the resilience and protection of critical infrastructure and key resources as evidenced by the existence of a myriad of legislation and policy currently in force. Emergency managers maintain responsibilities for the safety and security of the communities they serve and many of their own authorities flow from the applicable legislation and policy governing the cybersecurity responsibilities directed at the public sector. This is an emerging topic for emergency managers whose profession was initially founded on addressing natural emergencies and disasters.

Yet the inclusion of this new threat and the commensurate professional discipline adjustments it necessitates are not foreign concepts for emergency managers. September 11, 2001 as a defining event required the calibration of the emergency management discipline to include greater focus on human-made threats than had previously been the case. Therefore, incorporation of cybersecurity resilience for CI/KR into existing emergency management practices and learning is another natural topical evolution in the discipline itself. Acknowledging the salience of the topic for emergency managers is nonetheless essential to any subsequent activities that would follow to address the issues and gaps as well as build greater resilience for CI/KR against cyber attacks.

The landscape of the topic itself is multifaceted and requires concerted efforts by emergency managers and their established networks of public safety and private sector professionals in order to effectuate change. The legal and policy aspects framing many of the issues within the topic are rather broad-ranging and complex. Furthermore, those very issues often involve subject matter expertise not possessed by emergency managers themselves. Specifically, challenges involving the Fourth and Fifth Amendments of the United States Constitution as well as associated case law, unproductive or contradictory policies, and the mechanisms through which the latter are achieved are significant influencers in shaping the current state of affairs that will impact emergency managers in their endeavors to address the overall topic.

Despite hindrances uncovered during the course of this research, emergency managers are well-equipped to facilitate inclusion of cybersecurity for CI/KR into their planning efforts through skills they possess and knowledge they can obtain. As with other emerging topics in the emergency management discipline, becoming familiar with the multitude of factors surrounding the topic requires both a commitment to education and a determination to incorporate the subject matter into existing responsibilities. As should be evident from the research herein, understanding the areas where the greatest resistance in the private sector dynamic may arise is critical for emergency managers to achieving success in their endeavors. Employing the recommendations derived from the analysis will further advance the maturity of the topic and the common body of knowledge from which emergency management practitioners can draw.

Supporting literature gives no sign of this issue diminishing in salience or complexity. Rather, cybersecurity threats to CI/KR will continue to rise in new and challenging ways. Emergency managers have the opportunity to address the topic proactively and influence both

the legal and policy landscape as well as strengthen the partnerships with private sector entities by familiarizing themselves with the issues and drawing upon their robust knowledge, skills, and experiences. Their efforts to improve the resilience of CI/KR against cyber attacks in their communities can markedly further the safety of citizens and the infrastructure and assets upon which the country relies to support its way of life and livelihoods. This topic reflects a natural evolution of the emergency management body of knowledge and enables practitioners to demonstrate their continued relevance and added value in the face of a regularly changing threat landscape and the accompanying legal and policy mandates.

References

6 U.S.C. §§121-122 (2006).

6 U.S.C. §§131-133 (2006).

6 U.S.C. §321m (2007).

6 U.S.C. §§441-444 (2006).

American Public University System (APUS). (n.d.). *Master of Science in cybersecurity studies: Emergency management perspectives on cybersecurity*. Retrieved from http://www.apu.apus.edu/academic/programs/degree/1604/master-of-science-in-cybersecurity-studies

Arquilla, J., & Ronfeldt, D. F. (2001). *Networks and netwars: The future of terror, crime, and militancy*. Santa Monica, Calif.: Rand, 2001.

Auerbach, C. F., & Silverstein, L. B. (2003). *Qualitative data: An introduction to coding and analysis*. New York, New York: New York University Press.

Boyd v. United States, 116 U.S. 616 (1886).

Carroll v. United States, 267 U.S. 132 (1925).

Clayton, M. (2011, March). The new cyber arms race. *Christian Science Monitor*. Retrieved from http://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race

Comey, J. B. (2014, February 26). The FBI and the private sector: Closing the gap in cyber security [Video file]. Retrieved from http://www.rsaconference.com/videos/121/the-fbi-and-the-private-sector-closing-the-gap-in

Creswell, J. W. (2009). *Research design, qualitative, quantitative, and mixed methods approaches* (3rd ed.). Thousand Oaks, CA: Sage.

Daskapan, S. & Van der Berg, J. (2011). Designing cyber warfare information infrastructure resilience. Retrieved from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1042&context=isw

Department of Homeland Security (DHS). 2011. *Risk Management Fundamentals: Homeland Security Risk Management Doctrine*. Washington, D.C.: Department of Homeland Security, 2011.

Department of Homeland Security (DHS). (2013a). Critical infrastructure sectors. Retrieved from http://www.dhs.gov/critical-infrastructure-sectors

Department of Homeland Security (DHS). (2013b). Homeland Security Presidential Directive 7: Critical infrastructure identification, prioritization, and protection. Retrieved from http://www.dhs.gov/homeland-security-presidential-directive-7

Department of Homeland Security (DHS). (2013c). National Infrastructure Protection Plan. Retrieved from http://www.dhs.gov/national-infrastructure-protection-plan

Doe v. Holder, 703 F. Supp. 2d 313 (2010).

Geers, K. (2010). The cyber threat to national critical infrastructures: Beyond theory. *Journal of Digital Forensic Practice*, *3*(2-4), 124-130. doi:10.1080/15567281.2010.536735

Genge, B. B., Siaterlis, C. C., & Hohenadel, M. M. (2012). Impact of network infrastructure parameters to the effectiveness of cyber attacks against industrial control systems. *International Journal of Computers, Communications and Control*, *7*(4), 673-686.

Glick, S. J. (2012). Virtual checkpoints and cyber-Terry stops: Digital scans to protect the nation's critical infrastructure and key resources. *Journal of National Security Law and Policy*, *6*, 97-134.

Haddow, G., Bullock, J., & Coppola, D. (2011). *Introduction to emergency management*. (4th ed.). Burlington, MA: A Butterworth-Heinemann Title.

Homeland Security Act of 2002, 6 U.S.C. § 2 *et seq.*

Hunter, N. D. (2009). *The law of emergencies: Public health and disaster management*. Burlington, MA: Butterworth-Heinemann.

Jenelius, E., Westin, J., & Holmgren, Å. J. (2009). Critical infrastructure protection under imperfect attacker perception. *International Journal of Critical Infrastructure Protection*, *3*(1), 16-26. doi:10.1016/j.ijcip.2009.10.002

Kelly, T. K., & Hunker, J. (2012). Cyber policy: Institutional struggle in a transformed world. *I/S: A Journal of Law and Policy for the Information Society, 8*(2), 210-242.

Kochan, D. J. (1998). 'Public use' and the independent judiciary: Condemnation in an interest-group perspective. *Texas Review of Law and Politics*, *3*(1), 49-116.

Lin, H. (2012). Thoughts on threat assessment in cyberspace. *I/S: A Journal of Law and Policy for the Information Society*, *8*(2), 337-355.

Locke, L. F., Spirduso, W. W., & Silverman, S. J. (2007) *Proposals that work: A guide for planning dissertations and grant proposals* (5th ed.). Thousand Oaks, CA: Sage.

MacCarthy, M. (2012). Government and private sector roles in providing information security in the U.S. financial services industry. *I/S: A Journal of Law and Policy for the Information Society*, *8*(2), 243-276.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: A sourcebook of new methods*. Thousand Oaks, CA: Sage.

Miller, R. A. (2011). Cyber war realities - what lies ahead. *International Journal of Critical Infrastructure Protection*, *5*(2), 84-85. doi:10.1016/j.ijcip.2011.08.003

Obama, B. (2013). Presidential Policy Directive—Critical Infrastructure Security and Resilience. *Daily Compilation of Presidential Documents* (February 12).

Rice, M., Miller, R., & Shenoi, S. (2011). May the US government monitor private critical infrastructure assets to combat foreign cyberspace threats?. *International Journal of Critical Infrastructure Protection, 4*(1), 3-13. doi:10.1016/j.ijcip.2011.02.001

Rittel, W. J. R & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Policy Sciences, 4*(2), 155-169.

Rosenzweig, P. (2010). The organization of the United States government and private sector for achieving cyber deterrence. In National Research Council (Ed.), *Deterring cyber attacks: Informing strategies and developing options for U.S. policy* (pp. 244-269). Washington, D.C.: National Academies Press.

Saldaña, J. (2013). *The coding manual for qualitative researchers*. Los Angeles, California: Sage Publications, Inc., 2013.

Saxer, S. (2005). Government power unleashed: Using eminent domain to acquire a public utility or other ongoing enterprise. *Indiana Law Review, 38*(1), 55-102.

Singer, P. W. & Friedman, A. (2013). *Cyber security and cyberwar: What everyone needs to know*. New York, New York: Oxford University Press, 2013.

Sylves, R. T. (2008). *Disaster policy and politics, emergency management and homeland security*. Washington, D.C.: Cq Pr.

United States v. Odland, 502 F.2d 148, 151 (1974).

United States v. Ramsey, 431 U.S. 606, 615-616 (1977).

USA PATRIOT ACT of 2001, 42 U.S.C. § 5195c(e) *et seq.*

U.S. Census Bureau. (2013). *Computer and internet use in the United States: Population characteristics* (U.S. Census Bureau Publication No. P20-569). Retrieved from http://www.census.gov/prod/2013pubs/p20-569.pdf

U.S. Const. amend. IV.

U.S. Const. amend. V.

Vasilescu, C. (2012). Cyber attacks: Emerging threats to the 21st century critical information infrastructures. *Obrana A Strategie*, *12*(1), 53-63.

Young, M. D. (2012). United States government cybersecurity relationships. *I/S: A Journal of Law and Policy for the Information Society*, *8*(2), 278-320.

Zhang, Z. (2011). Cyberwarfare implications for critical infrastructure sectors. *Homeland Security Review*, *5*(3), 281-295.