DEFENSE SUPPORT TO CIVIL AUTHORITIES DOCTRINAL SHORTFALLS DURING CYBER ATTACKS

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
Strategic Studies

by

THOMAS T. BULLER, MAJOR, US ARMY
B.S., United States Military Academy, West Point, New York, 2007

Fort Leavenworth, Kansas
2018

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 15-06-2018	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From - To)* AUG 2017 – JUN 2018

4. TITLE AND SUBTITLE Defense Support to Civil Authorities Doctrinal Shortfalls during Cyber Attacks	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Thomas, T. Buller, Major, U.S. Army	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301	**8. PERFORMING ORG REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

As doctrine continues to evolve towards multi-domain battle, the homeland is under increasing risk. In the multi-domain extended battlefield, US reliance on the defense industrial base and strategic lines of communication present adversaries with unique opportunities. At the same time, access to domestic critical infrastructure and key resources in the cyber domain could put the homeland in play in the next war. Efforts to protect the nation's infrastructure in the cyber domain currently remain largely focused on cyber-defense. What if a threat actor successfully penetrated cyber-defenses and impacted critical infrastructure? What would the defense response look like if this attack came during a major combat operation? Would such an attack be defense support to civil authorities (DSCA) or homeland defense (HD), and does it matter? This thesis explores these questions by analyzing the current DSCA doctrine and comparing it to current cyber threats.

15. SUBJECT TERMS
Defense Suport to Civil Autority, Homeland Defense, Cyber, Critical Infrastrcture, National Security, Homeland

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	78	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: MAJ Thomas T. Buller

Thesis Title: Defense Support to Civil Authorities Doctrinal Shortfalls During Cyber Attacks

Approved by:

____, Thesis Committee Chair
DeEtte Lombard, M.A.

____, Member
Richard Berkebile, Ph.D.

____, Member
MAJ Justin Horgan, M.A.

Accepted this 15th day of June 2018 by:

____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

DEFENSE SUPPORT TO CIVIL AUTHORITIES DOCTRINAL SHORTFALLS DURING CYBER ATTACKS by Major Thomas T. Buller, 78 pages

As doctrine continues to evolve towards multi-domain battle, the homeland is under increasing risk. In the multi-domain extended battlefield, US reliance on the defense industrial base and strategic lines of communication present adversaries with unique opportunities. At the same time, access to domestic critical infrastructure and key resources in the cyber domain could put the homeland in play in the next war. Efforts to protect the nation's infrastructure in the cyber domain currently remain largely focused on cyber-defense. What if a threat actor successfully penetrated cyber-defenses and impacted critical infrastructure? What would the defense response look like if this attack came during a major combat operation? Would such an attack be defense support to civil authorities (DSCA) or homeland defense (HD), and does it matter? This thesis explores these questions by analyzing the current DSCA doctrine and comparing it to current cyber threats.

ACKNOWLEDGMENTS

My Command and General Staff College Master of Military Arts and Sciences Committee members provided incredible support, guidance, and insight that made this thesis possible. My Committee Chair, Ms. DeEtte Lombard, who also served as my Staff Group Advisor, helped me accomplish this thesis by improving my writing, guiding my process, and coordinating with the Committee. Dr. Richard Berkebile provided critical support to my research methodology, presentation of findings, and subject matter expertise on homeland security. Major Justin Horgan served as the cyber subject matter expert for this thesis, and greatly assisted in forming the introduction and completing the literature review. This expert team leveraged a unique mix of academic and professional expertise that allowed me to explore this important topic. I am deeply grateful for their time, energy, and patience.

Throughout my career I have been fortunate to have mentors that developed me as an officer and an individual. My mentors at the United States Military Academy imparted academic discipline in me, and taught me the importance of seeking knowledge in diverse fields of study. My leaders in the 101st Airborne Division continued to develop my professional competency and afforded me numerous unique experiences that molded my character. Before attending the Command and General Staff College, my mentors at Fort Benning taught me how to achieve work-life balance. Without these mentors in my life, I would not have the capability to complete a Graduate Degree Program.

Finally, my family provides me with essential support and motivation to seek new challenges and achieve great things in the military. My wife is the rock of my family, who balances her endeavors with raising our children and supporting our military

journey. Without her, long hours of research and writing would be impossible. My children, despite being young, have embraced military life and give me motivation to seek great things. Additionally, my extended family, to include parents, grandparents, and siblings, have all lent support that helped me achieve the balance required to complete this thesis.

TABLE OF CONTENTS

ACRONYMS

ADP	Army Doctrine Publication
ADRP	Army Doctrinal Reference Publication
APT	Advanced Persistent Threat
ASPG	Army Strategic Planning Guidance
ATP	Army Techniques Publication
CBRN	Chemical Biological Radiological and Nuclear
CIKR	Critical Infrastructure and Key Resources
COG	Continuity of Government
COO	Continuity of Operations
CYBERCOM	Cyber Command
DCI	Defense Critical Infrastructure
DoD	Department of Defense
DOTMLPF-P	Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities, and Policy
DSCA	Defense Support to Civil Authorities
FEMA	Federal Emergency Management Agency
FM	Field Manual
HD	Homeland Defense
NDS	National Defense Strategy
NERC	North American Energy Reliability Corporation
NMS	National Military Strategy
NRF	National Response Framework
NSS	National Security Strategy

SCADA	Supervisory Control and Data Acquisition
S-LOCs	Strategic Lines of Communication
SWIFT	Structured What-if Technique
USCERT	United States Computer Emergency Readiness Team

ILLUSTRATIONS

Page

TABLES

Page

CHAPTER 1

INTRODUCTION

> I am telling you all, this is the defense mission of the next century—homeland defense, fair and simple. It will take several different forms. Protection against terrorist attacks using chemical or biological weapons. Protection against attacks, cyber[space] attacks from people using computers to bring down air traffic control systems or utility systems or whatever. And homeland defense against world errant nations using a ballistic missile or two. So, homeland defense is the mission of the next century.
>
> —The Honorable John J. Hamre, Deputy Secretary of Defense

These comments from the Honorable John Hamre in 1998 offer a sobering view of the challenges facing the homeland and the military. Nearly 20 years after this statement, that sobering prophesy is reality. The terrorist attacks on the 11th of September 2001 completely took the nation's response capability by surprise and led to sweeping changes in government and defense. Individuals inspired by radical ideologies continue to commit acts of terror in the homeland despite these sweeping changes. Ballistic missile threats also remain a top concern as access to missile technology and weapons of mass destruction continue to expand. Iran and North Korea today represent two belligerent states that threaten the use of these missiles against the homeland. However, despite this security environment, these nations have not actually attacked the homeland with missiles, and terrorists have not been able to execute a catastrophic attack since September 11th. Based on recent reporting, Deputy Secretary Hamre's third prediction of cyber-attacks against the nation's critical infrastructure appears to be moving towards a dangerous realization. Assessments from the United States Computer Emergency Readiness Team (US-CERT) validate these concerns indicating numerous and ongoing cyber-attacks against critical infrastructure, including the energy sector, aviation, and public utilities (US-CERT 2017).

Studying the Department of Defense (DoD) concept of active layered defense in the homeland begins to frame the problem. Assuming the threats identified by Deputy Secretary Hamre remain preeminent, the current system for active layered defense favors airspace defense and chemical, biological, radiological, and nuclear (CBRN) defense. The DoD employs a full range of Doctrine, Organization, Training, Material, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P) solutions to defend against airspace and CBRN threats and to manage consequences. For example, CBRN defense starts far outside the US with counter-proliferation operations. This effort includes everything from reducing CBRN stockpiles globally to conducting strikes to dissuade users of CBRN weapons. Layered defensive measures to directly protect the homeland overlap overseas efforts with active surveillance, and interagency cooperation to defeat threats before they manifest. If these measures fail to stop an attack, the DoD maintains an entire enterprise of capabilities dedicated to responding to a CBRN incident in the homeland (National Guard Bureau 2016).

Comparing the CBRN problem set against the cyber problem starkly contrasts consequence management capabilities. The federal cyber-security enterprise responsible for protecting the nation includes interagency partners from across the government, including the DoD. Within the DoD, the US Cyber Command (CYBERCOM), specifically the Cyber National Mission Force, retains the responsibility to defend the nation’s critical infrastructure when consequences may include significant impacts (Department of Defense 2016).

In the last decade, CYBERCOM's efforts to protect the nation have contributed greatly to collective cyber-security. Remarkably, the command achieved this capability while also developing the force from nearly nothing. Returning to the hypothetical attack Deputy Secretary Hamre predicted in 1998, how would CYBERCOM manage the consequences of a successful cyber-attack on the nation? Based on existing frameworks, if a threat actor launched cyber-attacks on air traffic control systems and utilities, the Cyber National Mission Force would detect the threat, and in concert with other federal agencies, block the attack. Then CYBERCOM would use offensive capabilities to maneuver and defeat the threat (Department of Defense 2016). This series of actions parallels most of the CBRN response enterprise. However, what part of the cyber-security enterprise takes over if the CYBER NATIONAL MISSION FORCE fails to detect and block an attack? Currently, the management of any impact to critical infrastructure falls within the responsibility of Department of Homeland Security based on the National Response Framework (NRF). The DoD contributes to the NRF by providing both National Guard, Active Duty, and Reserve forces as part of a tiered response. Unlike the comprehensive system established to manage CBRN response, as of yet there is no enterprise approach to managing all aspects of a cyber-attack on critical infrastructure and key resources (CIKR).

Vulnerability of Critical Infrastructure

Part of the problem with ensuring comprehensive cyber-security relates to the vulnerability of the nation's CIKR. CIKR is an all-encompassing term that includes US national assets essential for security, safety, and our way of life (Department of Homeland Security 2009). These assets include power generation and distribution, public utilities, telecommunications, transportation, and manufacturing. A subset of CIKR, DoD specific assets, referred to as Defense Critical Infrastructure overlap within some sectors. An example of this overlap is critical defense manufacturing referred to as the Defense Industrial Base. One vulnerability of the nation's CIKR is that most of the assets are publically owned and operated (Department of Homeland Security 2009). Also, many of these CIKR assets connect in some way to the internet to ensure efficiency by automating controls, reducing the number of humans in the loop, and centralizing system monitoring. As publicly owned and operated assets, many of these CIKR nodes exist outside the protection of the federal or DoD networks. Though DHS, and in some cases CYBERCOM, operate in public networks to defend CIKR, the number of potential access points makes comprehensive security a daunting task. The sheer number of nodes in cyberspace convey how daunting this task is. Estimates from 2013 place the number of web pages on the internet at 30 trillion with nearly nine billion devices connected (Singer and Friedman 2014, 2). With each of these devices and web pages presenting a potential attack vector, DHS and CYBERCOM cannot be expected to detect and stop many of these attacks.

The success of the Stuxnet virus offers insight into the vulnerabilities of CIKR. This virus caused physical damage the centrifuges in an Iranian uranium enrichment facility and represented one of the most publicized cyber-attacks against critical infrastructure. The Stuxnet virus entered the Iranian network and compromised Supervisory Control and Data Acquisition (SCADA) systems. In this attack, the virus specifically targeted Programmable Logic Controllers commanding centrifuges to spin out of control while reporting normal operations back to the human interface (Singer and

Friedman 2014, 15). Many CIKR assets today utilize SCADA to automate critical processes. These systems remain vulnerable to attack even with man-in-the-loop analog backups and traditional cyber-security like firewalls. The Iranian system, for example, was air-gapped, meaning that it did not interface with the world wide web, but Stuxnet still made it onto the network (Singer and Friedman 2014, 63).

Today, Advanced Persistent Threats (APTs) represent the next generation of cyber threats to CIKR. APTs consist of the combined efforts of trained individuals, cyber tools, and techniques. APT threat groups seek to penetrate networks, expand laterally, seize SCADA controls, and ultimately deliver a viral payload to seize information, damage the system, or destroy physical components of a system that interface with the network. These threats may remain dormant in systems for long periods of time, and evade detection by design. US-CERT reports of APT activity in the SCADA systems of domestic CIKR raise serious concerns (US-CERT 2017).

Multi-Domain Battle Concept

The most recent update to Army Field Manual (FM) 3-0, *Operations*, paints a picture of future war where APT cyber-attacks will become the norm. In the multi-domain battle concept, adversaries will seek to gain positional advantage in any domain, and in any location (Department of the Army 2017). On the multi-domain battlefield of the near future, a full-scale cyber-attack against domestic critical infrastructure is likely, and serves to place the United States in a dilemma. If the U.S. is involved in large-scale combat operations abroad, and the CYBER NATIONAL MISSION FORCE fails to stop catastrophic cyber-attacks, who is responsible for consequence management in the homeland?

Problem

With the rapidly increasing size of cyberspace, the interface of critical infrastructure to the internet, and the employment of cyber-weapons against infrastructure, the United States faces a significant problem. Proliferation of dangerous cyber-weapons to many threat actors further compounds the problem for the US. In the current environment, the vulnerability of US CIKR to cyber-attacks, and the reports of early APT activity in multiple critical sectors, provide strong evidence that domestic CIKR will come under attack and fail catastrophically. Given the means exist to attack the nation's CIKR, I believe no actor currently possesses the motive and opportunity to do so. However, the multi-domain battle concept presents a situation where adversaries will have the means, motive, and opportunity to conduct such an attack. Adversaries facing the US in a multi-domain war have access to advanced cyber-weapons, that would catastrophically damage CIKR exposed to cyberspace, and would logically do so to offset US strategic reach and degrade force projection capabilities. Further, many adversaries may need to rely on this capability as the only means to offset traditional US strengths.

Hypothesis

Based on this problem, and the identified lack of comprehensive consequence management options, I believe that there are DOTMLPF-P gaps in the enterprise. I hypothesize that there is a shortfall in Defense Support to Civil Authorities (DSCA) doctrine related to response during a cyber-attack. Though other shortfalls may exist in the enterprise, this thesis does not examine them.

Primary Research Question

Do gaps exist in Army DSCA doctrine that would jeopardize national interests during a large scale cyber-attack on the homeland? The United States Army defines doctrine as "fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives" (Department of the Army 2016, 1-31). After framing the problem, and identifying some of the challenges multi-domain battle presents to DSCA execution, is there a lack of fundamental guiding principles for military forces?

Assumptions

Three critical assumptions frame this study. First, cyber-security and cyber-defenses will fail at some point during a future attack on domestic CIKR. This assumption is valid based on proven capabilities of threat actors and current threat reporting. Second, in the next large-scale combat operation, adversaries will both directly and indirectly conduct significant cyber-attacks against domestic critical infrastructure. This assumption is valid based on threat doctrine such as Russian New-Generation Warfare. This emerging Russian doctrine supports wide ranging cyber-attacks against both traditional military and critical civilian targets (Chekinov and Bogdanov 2018, 18-20). Third, the Army will use current DSCA doctrine to guide their actions during any cyber-attack impacting CIKR. This final assumption is valid based on the current legal definitions of DSCA, and the lack of alternatives to guide the Army's response. All three of these assumptions are necessary based on the chosen methodology, testing current doctrine against emerging and future threats.

Definitions and Terms

The following definitions and terms help to explain principles critical to the thesis. These definitions provide clarity and a common understanding of technical subjects, as well as emerging concepts.

Advanced Persistent Threat (APT): A sophistical and lengthy cyber-attack effort, led coordinated team of experts. APT attacks include stealthy intrusion, long term presence in a network, and the ability to deliver a cyber-attack (Singer and Friedman 2014, 293)

Critical Infrastructure and Key Resources (CIKR): Critical assets that ensure security and way of life. These assets often include utilities, communication, and transportation (Singer and Friedman 2014, 294).

Cyber-attack: In this thesis, a cyber-attack is any offensive activity in cyberspace designed to impact the network and nodes of a sovereign nation.

Cyber-defense: In this thesis, cyber-defense includes the activities of a nation to defend their networks and nodes against cyber-attacks.

Cyber-warfare: In this thesis, the interaction of cyber-attacks and cyber-defense between two or more belligerent nations.

Industrial Control System: An interface between a network that monitors and controls industrial processes (Singer and Friedman 2014, 296).

Multi domain extended battlefield: The extension of the modern battlefield into the homeland through space and cyberspace (Department of the Army 2017).

Limitations

This study has several limitations. First, unclassified material and sources were used. The study focused on analysis of broad doctrinal concepts and open-source threat reporting to allow maximum dissemination. Second, the study did not use advanced modeling tools to model doctrinal systems or threats. Finally, this study presented a qualitative analysis of the problem. Based on available time, tools available, and the nature of the question, a qualitative analysis best answered the primary research question.

Delimitations

This study answered a "does" question regarding current Army DSCA doctrine. I did not attempt to answer a "how" question. The study focused on current Army DSCA doctrine specifically Army Doctrine Publication (ADP) 3-28, Army Doctrine Reference Publication (ADRP) 3-28, and Army Techniques Publication (ATP) 3-28.1. This study will did not expand outside of the Army's doctrinal role in DSCA, and did not analyze the NRF, or other elements of DOTMLPF-P. Finally, this thesis is not a study of cyber-warfare, but rather incorporates cyber-warfare as it applies to DSCA.

Conclusion

As warfare changes, new problems will challenge doctrinal principles across the spectrum of operations. Problems that pose strategic challenges must be addressed sufficiently in doctrine. The speed of the next conflict will not allow for significant doctrinal changes in stride. It is critical to identify doctrinal shortfalls in times of relative peace to ensure refined principles guide the Army's actions in war.

The following chapters include a literature review, an overview of research methodology, a presentation of data, and final conclusions. The next chapter presents a summary of the current body of knowledge. I divided the literature into the categories of relevant cyber-war theories, strategic policy, the role of Army doctrine, previous studies on doctrinal shortfalls, and the current threat.

The third chapter reviews the research method used to answer the primary research question. This chapter reviews the genesis of the problem identification through hypothesis and research question formulation. The third chapter concludes with an explanation of the selected methodology to investigate the problem and the assessment criteria.

The fourth chapter applies the facts of the problem to the research methodology. This chapter presents answers to the research questions along with analysis of those findings. The final chapter then interprets those findings and presents recommendations for further study.

CHAPTER 2

LITERATURE REVIEW

Introduction

The purpose of this research thesis is to determine what shortfalls exist in Army DSCA doctrine based on evolving cyber threats. A careful and thorough literature review provided a framework for understanding the critical elements of the problem. I developed this understanding by examining the current body of knowledge related to the unique aspects of the problem. One of the challenges associated with researching an emerging threat included continual evolution of theory, and a limited number of proven paradigms. Taking this challenge into account, I examined a variety of scholarly sources with multiple points of view. Further, I also examined relevant official documents and broad foundational doctrine to fully frame the problem.

Organization

The review began from a broad theoretical and strategic perspective. The intent of this starting point was to build a base of understanding related to the most prevalent schools of thought on cyberwarfare, and its potential impact on the homeland. Building upon that strategic base, I then examined relevant literature at the operational and then tactical levels. With an understanding of the literature from the strategic to the tactical level. The most recent literature on the evolution of the threat followed. Organizing the review from strategic and theoretical to tactical rapidly built an overall understanding of the problem.

Groups of Relevant Literature

Grouping the literature into distinct categories scoped the body of knowledge down into the most relevant topics based on the organizational framework. Cyber-war theories from academic journals, strategic studies, and seminal works were examined. From this group theoretical works that commented on potential impacts to the homeland were selected. Examining multiple and opposing theories helped to control for bias. Before moving onto the operational and tactical level, the review then examined strategic policy which establishes national security priorities. The doctrinal review remained limited to only the purpose and definitions of Army doctrine. This limited doctrinal review set conditions for further investigation of Army DSCA doctrine in chapter four. After examining the purpose of doctrine, I then examined previous research on doctrinal shortfalls. The literature review concluded with current cyber threats. The intent was to familiarize the reader with the type of threats as a basis for the subsequent chapters.

Cyber-Warfare Theory

Cyberspace is a domain just like space, land, or the air. When technology gives humankind access to a new domain, nations quickly find ways to exploit that domain for defensive advantages. Important to the development of capabilities are theories regarding the use of force in that domain. For example, airpower theory developed after the First World War informed the development of strategic bombing and the creation of separate air forces. Based on the review of current literature, cyber-warfare theory includes everything from advocating strategic offensive postures to limiting cyberwarfare to defensive tactical activities.

Looking at the cyberwarfare scenarios impacting DSCA doctrine, the most important literature comments on cyber-warfare impacting CIKR. Two prevalent cyber-warfare theories emerge. The first school of thought argues that cyber-warfare is a strategic possibility that could impact CIKR. The counterpoint argues that cyber-warfare is inherently limited and could not significantly impact CIKR to the extent that it would create strategic level impact. It is important to note neither school disputes the fact that cyber-attacks can and will occur, and neither precludes cyber-attacks may evolve over time.

One theory on cyber-war posits that targeting an adversary's CIKR is both possible and inevitable. Several key factors make cyber-attacks on CIKR strategically viable. First, the use of cyber-war mitigates advantages possessed by an adversary. Researchers on Chinese cyber-war capability development quickly highlight that this approach falls in line with Chinese concepts for unrestricted warfare (Muniz 2009, 58). Developed nations, specifically western nations, remain vulnerable to the effects of cyberwar due to the interdependence of their CIKR and the internet. Additionally, the limited barriers to entry provide weaker rival nations with potential parity in an entire domain (Muniz 2009, 25). Further, nations wishing to avoid a direct military conflict may strategically use cyberwar when combined with other defenses (Libicki 2009, 122).

Most theorists agree that cyberwar is not decisive on its own and must be combined with other more traditional forms of warfare to achieve strategic impacts (Libicki 2009, 137). However, cyberwar when used in conjunction with operational campaigns or tactical actions achieve decisive operational impact. Cyber-attacks on critical infrastructure may disrupt or degrade an enemy's command, control, and communication, providing decision-making advantages and surprise (Muniz 2009, 60). In the current environment, disruptions of national command, control, and communications infrastructure provide all the time necessary for an adversary to gain an operational or tactical position of advantage. This advantage may prove strategic in the onset of hostilities if it renders a nation unable to respond. The possibility of anonymity and murky legal lines further compound the disruptive effects of a cyber-attack on critical infrastructure (Muniz 2009, 25).

One of the strongest arguments from this school of thought provides historic examples of these key factors. For example, Russian cyber-attacks coordinated with tactical actions in August of 2008 proves the reality of cyberwar. Russian DDoS attacks on Georgian networks coordinated with the movement of troops and air strikes created enough confusion to degrade Georgian situational understanding (Connell and Volger 2017, 18). Recall the example of the Stuxnet virus that broke ground by ultimately delivering a payload to cause physical damage to Iranian centrifuges. More recently, theorists point to a Russian cyber-attack on December 23, 2015 on the Ukrainian electrical grid. This sophisticated and coordinated attack relied on extensive reconnaissance, hijacking of SACDA to turn off the power, malware destruction of files, and DDoS attacks to amplify the effects of the attack (Connell and Volger 2017, 20). Further adding to their argument, forensic analysis of the attack showed that the intruders could have permanently damaged power generation infrastructure but chose not to (Connell and Volger 2017, 20).

The other cyber-warfare theory contends that cyber-attacks have will not strategically impact critical infrastructure. Several key factors support this theory.

Theorists writing prior to 2015 argue that attacks on CIKR have not occurred, even if theoretically possible. A quantitative analysis of cyber-attacks from 2001 to 2011 highlighted that open-source reported incidents remain relatively low, and typically involve espionage or information collection (Valerino and Maness 2014, 357-358). Many of these theorists place the STUXNET attack into the cyber espionage category or treat the event as an outlier.

Stronger arguments against strategic effects involve more traditional theories of war and international relations. Interestingly, both schools of thought tend to agree that cyber-warfare by itself is not decisive. The camp against strategic cyber-warfare sees several key flaws in cyber-attacks. First, to achieve strategic impact, effects would need to be decisive and long-term. As cyber-weapons typically rely on an unknown exploitation, once the weapon is used, counter measures immediately close the vulnerability rendering the weapon obsolete (Gartzke 2013, 60). Second and third order effects further limit the use of cyber-weapons based on this "one and done" principle. First, once a weapon is used, it can be reverse-engineered for use against the original attacker. Further, the cost effectiveness of anything that is "one and done" inherently limits government investment (Boyd 2009).

Additionally, without knowing who is responsible, no one can force their will on their adversary (Gartzke 2013, 49). This argument asserts anonymous cyber-warfare is effectively a means without ends, rendering it strategically flawed. One of the strongest arguments against strategic cyber-warfare involving CIKR involves the possibility of uncontrollable escalation. The literature highlights the potential for escalation in the cyberspace as well as across other domains. Theorists argue the use of a cyber weapon against an adversary's CIKR invites the same type of attack in kind (Libicki 2015, 52). The nature of technology proliferation creates a paradox where the most capable of conducting cyber-attacks remain also the most vulnerable (Libicki 2015, 52). Further, nations most vulnerable to a CIKR attack remain the most capable of striking back physically, limiting targets only to nations that cannot strike back in any domain (Gartzke 2013, 65).

In summary, two predominant schools of thought take the opposite points of view regrading strategic cyber-attacks on CIKR. The camp arguing it is possible highlights the capability exists, it may be the only way to contest a dominant power, and may provide decisive advantages when combined with other operations. The counter position argues cyber-warfare is by itself remains indecisive, strategically flawed, and may escalate a situation well outside the intended effects. However, two critical pieces of common ground unite both camps. Neither camp denies that cyber-attacks will continue, and neither camp predicts that strategic cyber-warfare is not possible in the future.

Policy

Analysis of current policy positions of the United States Army, National Guard Bureau, and the United States Army Reserve puts current DSCA doctrine into perspective. Policy related literature starts with the National Security Strategy (NSS) and nests down to Army Policy. Similar to the review of cyber-warfare theory, the policy examination focused on the issues related to the primary research question. Specifically, this review examined the policy position of the United States Government and the Army regarding cyberattacks on critical infrastructure and interrelated DSCA issues.

The *National Security Strategy* (NSS) *of the United States* from December of 2017 clearly identifies both the importance of CIKR protection and the threat posed by cyber-attacks. Its first pillar is entitled "Protect the American People, the Homeland, and the American Way of Life" (U.S. President 2017, 7). The policy prioritizes the importance of federal response during attacks on the homeland as well as resilience through continuity of government. Communication networks, the electrical grid, the financial sector, military command and control systems, transportation networks, and the health system are identified as strategic vulnerabilities (U.S. President 2017, 13). The policy directs government efforts to combatting areas where cyber-attacks create catastrophic or cascading effects (U.S. President 2017, 13).

Analysis of this capstone policy reflects the cyberwar theory that projects the possibility of CIKR attacks on the homeland. Absent at this high level of policy, however, is the military role in combatting this threat, or responding to attacks on the homeland. The key takeaway is that protection of the homeland, specifically vulnerable critical infrastructure, remains the number one priority of the president.

The summary of the National Defense Strategy (NDS) dated 2018 reflects the position of the DoD and nests with the NSS. It echoes the concerns of the NSS specifically naming Russia, China, North Korea, and Iran as strategic competitors seeking to contest vital United States national interests in all domains (Department of Defense 2018, 1). The most important highlight from the NDS is the "homeland is no longer a sanctuary" and that "during conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated" (Department of Defense 2018, 3).

The *National Military Strategy* (NMS) informs how the Joint Force achieves the enduring national security interests outlined in the NSS. The 2015 NMS again prioritizes the survival of the nation, and prevention of a catastrophic attack on the homeland as the top two priorities (Chairman, Joint Chiefs of Staff 2015, 5). Despite being nearly three years removed from the current NMS and NDS, the NMS projects an identical strategic problem set. The key aspect of the problem emerges further into the NMS. Forward projection of military capability to deter, deny, and defeat threats is clearly the Chairman of the Joint Chiefs of Staff (CJCS) policy (Chairman, Joint Chiefs of Staff 2015, 7).

In the event of a major attack on the homeland, regardless of the domain, the Joint Force's priorities are security of global strike capabilities, maintenance of force projection capabilities across strategic lines of communication (S-LOGs), and full mobilization of National Guard and Reserve forces to provide the required force depth to accomplish overseas missions. The division of labor during a full mobilization is not in the NMS, but defeating the threat overseas with the total Joint Force links ends, ways, and means.

Army Strategic Planning Guidance (ASPG) from 2014 continues with the realization that the Army's mission is to provide expeditionary land combat power to the Joint Force. The APSG emphasizes use of the Total Army to meet future threats depth (Department of the Army 2014b). The Total Army concept includes the active duty Army, the Army Reserve, and the Army National Guard to meet operational requirements. Under the Total Army, Army Reserve and National Guard units augment the active duty Army by providing low-density personnel, critical equipment, and additional general-purpose combat forces to round out deploying units. The guidance calls for increased use of the National Guard and Army Reserve for operational capabilities and strategic depth (Department of the Army 2014b, 12). At the same time, the ASPG calls for the Active Army to remain ready to conduct no notice DSCA leveraging their readiness and expeditionary capabilities to rapidly respond to domestic emergencies (Department of the Army 2014b, 6). Further, the ASPG improved DSCA access to the Army Reserve based on the provisions of the 2012 *National Defense Authorization Act*.

Examining the linked policy documents from the NSS down to the ASPG, two key assumptions existed before 2014 that no longer remain valid. First, the Army would execute DSCA *or* expeditionary combat operations. The single use of the term "homeland defense" in the ASPG is telling. Army Policy appears to treat these events as mutually exclusive. Second, policy governing the purpose of the National Guard and Army Reserve mirrors this dilemma. The same critical capabilities retained in the Army Reserve and National Guard that the Joint Force relies on during expeditionary combat operations provides domestic authorities essential support for DSCA. Examples of these capabilities include rotary aviation, CBRN, communication, logistics, and transportation.

It is important to highlight the most recent posture statements of the Army National Guard and Army Reserve. The NSS and NDS framed the vulnerability of CIKR to cyber-attack, and the expectation of attacks on the homeland in the future. The NMS outlined the operational approach to combat this threat through protection of CIKR related to force projection, and prioritization of defeating the threat with the full Joint Force. ASPG directs the Total Army to provide the backbone of land combat power to the Joint Force and immediately respond to DSCA when required. The National Guard meets this challenge with pledging an all-of-the-above solution by meeting all operational requirements as well as all domestic response missions (Army National Guard 2017, 4). The Army Reserve meets this challenge by dividing the force into an expeditionary ready reserve and "other units" for DSCA and Homeland Defense (HD) (U.S. Army Reserves 2017). How exactly the Total Army will accomplish both DSCA and expeditionary combat operations remains an open question.

The Purpose of Army Doctrine

Understanding the purpose and uses of Army doctrine helps frame a critical aspect of the research question. The most foundational Army documents include ADRP 1-02, *Operational Terms and Graphics,* and ADP 1-01, the *Doctrine Primer*. ADRP 1-01 serves as a dictionary for the Army. *Operational Terms and Graphics* provides a common definition to terms to ensure shared understanding across the Army. ADRP 1-02 defines doctrine as "fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application" (Department of the Army 2016b, 1-31).

Taking the key words "fundamental principles" from that definition I compared that explanation of what doctrine is to ADP 1-01. The *Doctrine Primer* builds on ADRP 1-02 defining "fundamental principles" as "comprehensive and fundamental rules or an assumption of central importance that guides how an organization or function approaches and thinks about the conduct of operations" (Department of the Army 2014a, 2-1).

These two documents narrowed the problem down to fundamental principles, rules, and assumptions that would govern DSCA actions. I used this understanding as part of the methodology to help model the doctrinal system. Foundational doctrine places critical importance on key principles as they underlie a doctrine's logical framework and remain nested throughout the hierarchy.

Previous Studies on Doctrinal Shortfalls

Previous research on cyber related DSCA doctrinal shortfalls examines cyber-defenses, continuity of operations, and proper roles for DSCA forces. Past research separates DSCA activity shortfalls from cyber-attacks on CIKR and does not make a full linkage between concepts. Research related to the proper role of DSCA forces are based on natural disasters or terrorism. DSCA research related to the cyber-threats do not examine the problem outside of cyber-defense.

The strategy and vision of the National Guard described in previous section is an "all the above" approach. The current policy position of the National Guard is to perform both DSCA tasks and operational deployments to standard. Obvious prioritization problems in readiness and matching correct capabilities result. This approach is not new, however, as pointed out in case studies, the Louisiana Army National Guard did not execute DCSCA during Hurricane Katrina since they were deployed to Iraq (Kirkland 2008, 61). The problem facing the Louisiana National Guard revolved around defining their role as an operational reserve or strategic response force (Kirkland 2008, 86-88). The same problem faces the Army Reserve, stuck in the horns of a dilemma between DSCA requirements and requirements to support the Joint Force with critical capabilities. This analysis is helpful; however, the recommendations do not take into account modern cyber-attacks against CIKR. As the NRF grows and builds efficiency every year, it appears that even events like Hurricane Katrina may be managed and scaled to limit impacts on the military. The size and scale of a cyber-attack on the CIKR of the nation could immediately overwhelm NRF capabilities.

CIKR attacks and military response literature favors continuity of operations (COO) responses. Examination of shows some principles that seem to align with NMS and ASPG priorities. The focus of the military during cyber-attacks should be ensuring force flow remains uninterrupted, and that force projection related infrastructure, along with military command and control, is reconstituted as soon as possible (Larson and Peters 2001, 123). This 2001 research used cyber-attack models from the 1990s, limited in scale and scope. However, despite using obsolete threat data, the conclusions match with NMS and ASPG guidance to protect force projection and defeat the threat.

Additional cyber specific DSCA research explores the proper role of Army Cyber forces performing DSCA missions. The National Missions Forces established from CYBERCOM retain the CIKR protection mission in the United States (Hopes 2013, 16-18). These forces protect aspects of the network, but do not have responsibilities outside the cyber domain. As established in cyber-warfare theory, cyber operations should be synchronized with other military operations to achieve decisive effects. Using this logic, defensive cyber missions should have a physical DSCA or HD component. Literature advocating for pairing cyber capability with other military activity however defaults to the establishment of this capability only for offensive operations outside the U.S. Again, this nests with NSS, NDS and ASPG guidance for fighting the threat overseas, but fails to account for impacts in homeland (Nakasone and Lewis 2017, 22).

Related research on shortfalls gets close to the problem posed in this research thesis, but does not put all the elements together. DSCA shortfalls research is based on strategic environment from the 1990s and 2000s. Current threats greatly magnify the problems identified in this previous research. Threats overseas today require the Total Army to meet the requirements of the Joint Force, while large scale cyber-attacks on CIKR could extend well outside military CI.

Current Threats

The final category reviewed compiled recent descriptions of the threats posed to CIKR from cyber-attacks. Due to the sensitive nature of vulnerability reporting, only open source reporting from authoritative sources were examined. The most informative literature included after action reporting from national level exercises, testimony before legislative bodies, and technical threat reporting from industry and government sources. Analysis is confined to topics involving the research problem. Severity and probability is covered in subsequent chapters.

As the nation updates aging CIKR more and more systems become connected through the internet. Though this builds efficiency and some resiliency, networking CIKR creates vulnerability to cyber-attack. Since the 2000's, the federal government began to execute exercises with CIKR partners to test system resiliency against cyber-attacks. Cyberstorm and Gridex represent two of the largest scale exercises involving CIKR. Analysis of after action reports from these exercises helps to frame the problem, and highlights the threat under realistic conditions.

Cyberstorm is a national level cyber-attack simulation exercise first conducted in 2006. Led by the Department of Homeland Security, Cyberstorm simulations include multiple partners from the interagency and the private sector. After action reports from 2006 to 2016 show improvements across the entire community in both mitigation and response. However, two important trends remain unanswered. As first outlined in Cyberstorm I, attacks across multiple CIKR sectors pose significant challenges to response and remain a significant vulnerability (Department of Homeland Security 2006, 2). Additionally, vulnerabilities increase significantly as more CIKR sectors become involved in simulations. In Cyberstorm V, the public health sector experienced significant difficulty managing attacks and synchronizing with federal agencies (Department of Homeland Security 2016, 2).

Gridex is a similar simulation executed by the North American Energy Reliability Corporation (NERC). Gridex specifically simulates cyber-attacks on the national power grid. Like Cyberstorm, subsequent Gridex reports show improvement in response and mitigation. However, one significant shortfall remains the ability to manage physical damage to infrastructure (NERC 2016, vi). NERC priorities clearly outlined in the after-action report from Gridex III place the restoration of power generation and transmission ahead of all other CIKR sectors. Analysis of these reports suggest that additional CIKR sectors should expect to remain disrupted for lengthy periods of time.

Testimony before the House Committee on Transportation and Infrastructure in 2016 by representatives from DHS and NERC further develops these threat assessments. First, authorities anticipate cyberattacks against CIKR, citing Ukraine as a “harbinger of things to come” (Government Publishing Office 2016, 3). Additionally, the impacts of a coordinated cyber-attack could impact CIKR from days to months depending on the size and scope of the attack (Government Publishing Office 2016, 3). Further, several response protocol assumptions may no longer be valid. First, with timelines involving energy infrastructure, any attacks that could potentially impact a State for more than 72 hours will trigger activation of the National Guard and federal aid requests (Government Publishing Office 2016, 5). More specifically it seems that the position of DHS and the energy CIKR sector frame all cyber-attacks under a DSCA scenarios without regard for state sponsored HD dimensions.

The most recent threat reporting suggests state actors continue to gain access to CIKR and possess the means necessary to execute a cyber-attack on the CIKR. In October of 2017, CERT posted a joint technical alert outlining recent operations from the Dragonfly APT Group targeting the energy sector (US CERT 2017). Forensic analysis conducted by Symantec, a computer security company, confirmed the operation successfully accessed the SCADA of several energy providers (Symantec 2017). Given the Dragonfly APT group is associated with Russian IP addresses, analysis suggests rivals retain a position to strike at CIKR using cyber weapons.

Summary

The literature identifies common threads throughout the current body of knowledge. These threads inform conclusions critical to continuing examination of the research problem. Examination of theory reveals that strategic cyber-attack against CIKR is possible even if only in concert with other actions. Threat reporting confirms this theory by highlighting successful CIKR attack is Ukraine as well as ongoing APT activity in U.S. CIKR. Recent strategic policy recognizes this threat and places defense of the homeland as the number one priority. Strategic military policy suggests expeditionary operations to deter, deny and defeat adversaries remains the number one priority for the

Army, and the best way to ultimately keep the homeland secure. The strategy of the Total Army echoes this guidance relying on the National Guard and Army Reserve as operational force providers. Despite doctrinal separation of DSCA and HD, cyberwar theory combined with current threat reporting indicate the line between the two is becoming increasingly unclear.

The literature indicates that significant cyber-attacks on the CIKR of the U.S. are possible, and recent APT activity indicates that at some point an attack would be probable. To further explore the research problem, both the doctrinal DSCA system and threat must be modeled and tested. In the following chapter, the thesis continues with outlining the full methodology.

CHAPTER 3

RESEARCH METHODOLOGY

Introduction

This chapter outlines the process to answer the primary and secondary research questions. This thesis is a qualitative study to determine doctrinal shortfalls based on an emerging threat. Determining doctrinal shortfalls based on emerging threats is difficult due to the complex nature of doctrine. The Army Doctrine Primer outlines doctrine five major types of information in doctrine: principles, tactics, techniques, procedures, and terms and symbols (Department of the Army 2014a, 2-1). Within the body of doctrine for a given subject, there can be hundreds of pages of information in a variety of combinations. Modeling a threat as broad as a cyber-attack adds to the difficulty of this task. Typically testing these types of threats requires computer simulations and detailed modeling requiring volumes of technical data. Based on the limitations of the study, I chose to use a simple risk management methodology, the what-if analysis, commonly used in industry. The American Chemical Society defines a what-if analysis as a brainstorming technique used to determine what can go wrong in a system presented with a specific hazard. This analytical framework helps to determine specific gaps in an existing system (American Chemical Society 2016). This technique is appropriate for simple research problems of complex systems and does not require advanced modeling tools (American Chemical Society 2016). Doctrine ultimately is a complex system of interconnected information that provides guidance. Principles and concepts network together in a series of nodes. Using overarching principles and concepts it is possible to model that system and test it against threats using a what-if analysis.

The Structured What-if Technique (SWIFT)

I selected a modified version of the what-if analysis to reduce the number of nodes in the doctrinal system and ensure efficiency. The Structured What-if Technique (SWIFT), structures what-if brainstorming around key parts of a system and realistic hazards. The SWIFT protocol begins with modeling the key nodes of the system. Then a team of experts typically develops broad categories of hazards on a checklist to further structure the analysis. Within these categories, team members ask what-if questions based on their experience and domain knowledge (Acquisition Safety and Environmental Management System 2017). Team members then use their judgement to assess how the system would react to those what if questions and identify shortfalls. A common example of this technique is identifying hazards in a chemical process in an industrial setting. Using SWIFT, the team would model the critical nodes of the industrial process to make a given chemical. The team would then select broad categories of questions such as human error or mechanical fault. Within these categories, the team then asks what-if questions such as “what if the main pipe breaks”. Using their knowledge of the system and the hazard, the team then determines the outcome of the what-if question and identifies any shortfalls.

Advantages

The SWIFT technique offers many advantages specifically related to this study. First, the methodology is highly efficient, specifically in terms of modeling something as complex as a body of doctrine. Using knowledge gained in the literature review, I structured the DSCA doctrinal system into a manageable set of critical nodes reducing the need for excessive iterations. Second, SWIFT is a flexible methodology used in several disciplines from industry to healthcare (Acquisition Safety and Environmental Management System 2017). Within the flexible SWIFT framework, once I modeled the doctrinal system, I modeled the cyber threat and determined a reasonable number of what-if questions based on information gathered in the literature review. Finally, I selected this methodology specifically based on feasibility. Despite the limitations of time and amount of technical information available, this methodology still produces qualitative results capable of answering the research question.

Disadvantages

Like any methodology, using SWIFT incurs several disadvantages. First, the methodology relies on expert domain knowledge to identify threats and apply judgment regarding shortfalls (Acquisition Safety and Environmental Management System 2017). I controlled for this disadvantage by conducting a literature review and utilizing official threat reporting to ensure realism of the what-if questions. Also, the methodology produces only qualitative results due to the refinement of both the system and the judgement used to develop what-if questions (Acquisition Safety and Environmental Management System 2017). As this study is a qualitative study of potential doctrinal shortfalls, the disadvantage is minimal.

Bias

The use of judgement to structure and model both the doctrine and the threat created the most significant bias. As evidenced in the literature review, two divergent schools of thought exist regarding the potential for a cyber-attack on CIKR. I utilized several techniques to reduce bias. First, I based this study on the assumptions that a future cyber-attack will defeat cyber defenses and impact CIKR, and cyber-attacks will be used by adversaries in a large-scale combat operation. I also assumed that DSCA doctrine would guide response during any cyber-attacks on the CIKR. With these assumptions beginning to control bias, I then modeled the critical nodes of the doctrinal system based on ADP 1-01. Second, based on information from authoritative sources, such as US-CERT, I modeled a realistic threat. With an authoritative model of DSCA doctrine, and a realistically modeled threat, the results of the study remain generally insulated against bias.

Primary Research Question

The primary research question is: do gaps exist in Army DSCA doctrine that would jeopardize national interests during a cyber-attack on the homeland? The key parts of the question highlight the specificity of the study. Specifically, the study sought to identify if a gap existed.

Secondary Research Questions

The answer to the primary research question relies on several secondary research questions. First, what does current Army doctrine say about responses during cyber-attacks on the nation? Answers to this question will help to model the DSCA system. Second, what are the most likely and most dangerous cyber-attacks scenarios? Answers to this question will help develop what-if questions to test the modeled DSCA system. Finally, is DSCA Doctrine are no longer valid based on the most dangerous and most likely scenarios. The answer to this question will identify if gaps in DSCA doctrine exist.

Process

The methodology began with identification of a problem based on emerging threats outlined in FM 3-0, academic journals, and in the media. The process continued by posing a hypothesis on that problem. The primary research question is a derivative of the hypothesis, sufficiently narrowed down to allow research and testing, within the limitations of the study. Data collection in the literature review provided a basis for the secondary research questions. Finally, I applied the SWIFT protocol to the problem set which answered the primary research question. The figure below outlines the initial broad research process.

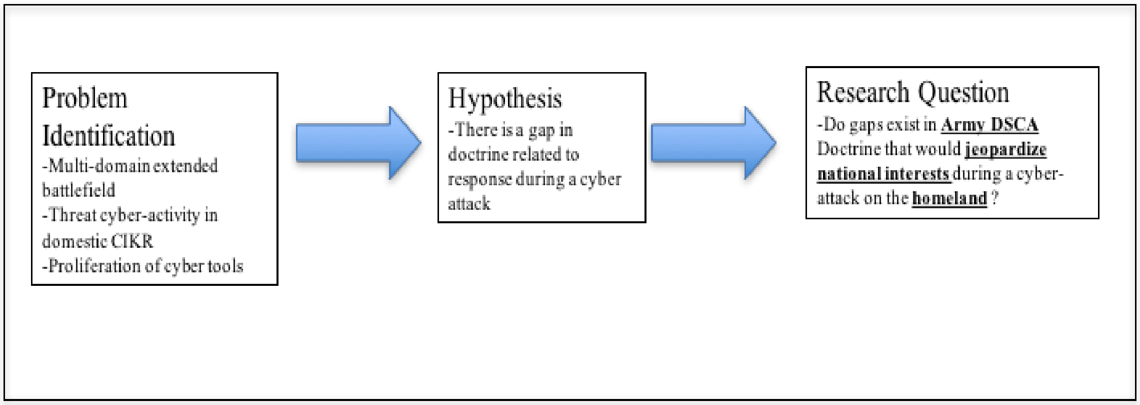

Problem Identification
-Multi-domain extended battlefield
-Threat cyber-activity in domestic CIKR
-Proliferation of cyber tools
Hypothesis
-There is a gap in doctrine related to response during a cyber attack
Research Question
-Do gaps exist in Army DSCA Doctrine that would jeopardize national interests during a cyber-attack on the homeland ?

Figure 1. Initial Research Process

Source: Developed by author.

Application of SWIFT

I applied the Structured What-if Technique to the problem in five steps, allowing sequential answers to the secondary research questions. In the first step, I selected the key nodes of the doctrinal system using criteria outlined in ADP 1-01 and ADRP 1-02, and cross referenced those nodes among DSCA doctrinal publications. The resulting nodal model of the doctrinal system is common to all publications, universally applicable, and of primary importance. This model established a framework to answer the secondary research question: what does current Army doctrine say about responses during cyber-attacks on the nation?

Following this step, I modeled the threat by creating a most likely and most dangerous scenario based. These two scenarios served as two independent "experiments" to test against the doctrinal system. Within each of these scenarios, I then developed three broad categories of what-if questions in accordance with SWIFT protocol. Structured brainstorming based on these categories yielded numerous what-if questions for each scenario. I chose the most relevant what-if question for each category, and in each scenario developing six total questions to test the doctrinal system. The three most likely questions served as variables in the most likely experiment, and the three most dangerous questions served as the variables in the most dangerous experiment. The doctrinal nodes served as the control for both experiments.

The fourth step compared the doctrine against the modeled threats by asking the what-if questions. In the final step, I used the hypothesis there is a doctrinal gap. With this assertion, I answered the what-if questions as true or false in relation to the hypothesis and provided justification for that answer. Chapter four presents aggregated, studied, and interpreted data from this process. The following figure graphically depicts the SWIFT process as it integrates primary and secondary questions.

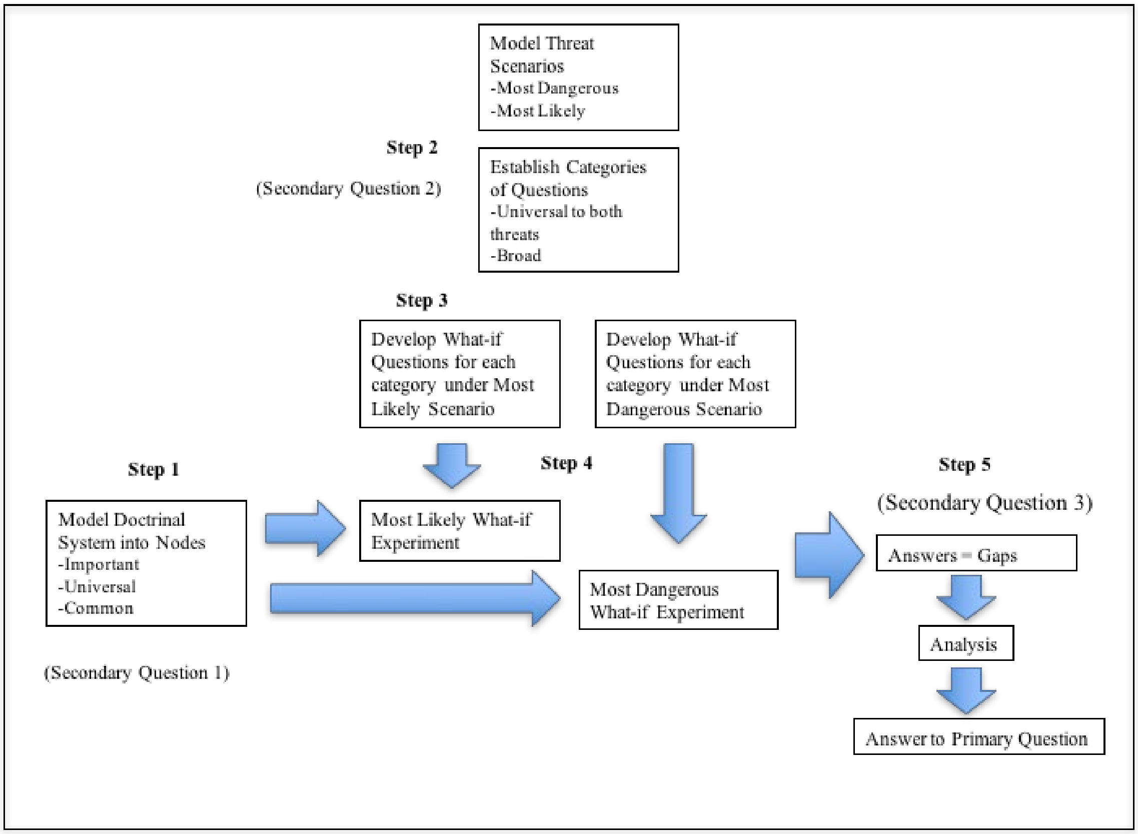

Model Threat Scenarios
-Most Dangerous
-Most Likely
Step 2
(Secondary Question 2)
Establish Categories of Questions
-Universal to both threats
-Broad
Step 3
Develop What-if Questions for each category under Most Likely Scenario
Develop What-if Questions for each category under Most Dangerous Scenario
Step 1
Model Doctrinal System into Nodes
-Important
-Universal
-Common
(Secondary Question 1)
Most Likely What-if Experiment
Step 4
Most Dangerous What-if Experiment
Step 5
(Secondary Question 3)
Answers = Gaps
Analysis
Answer to Primary Question

Figure 2. Structured What-if Technique Application

Source: Developed by author.

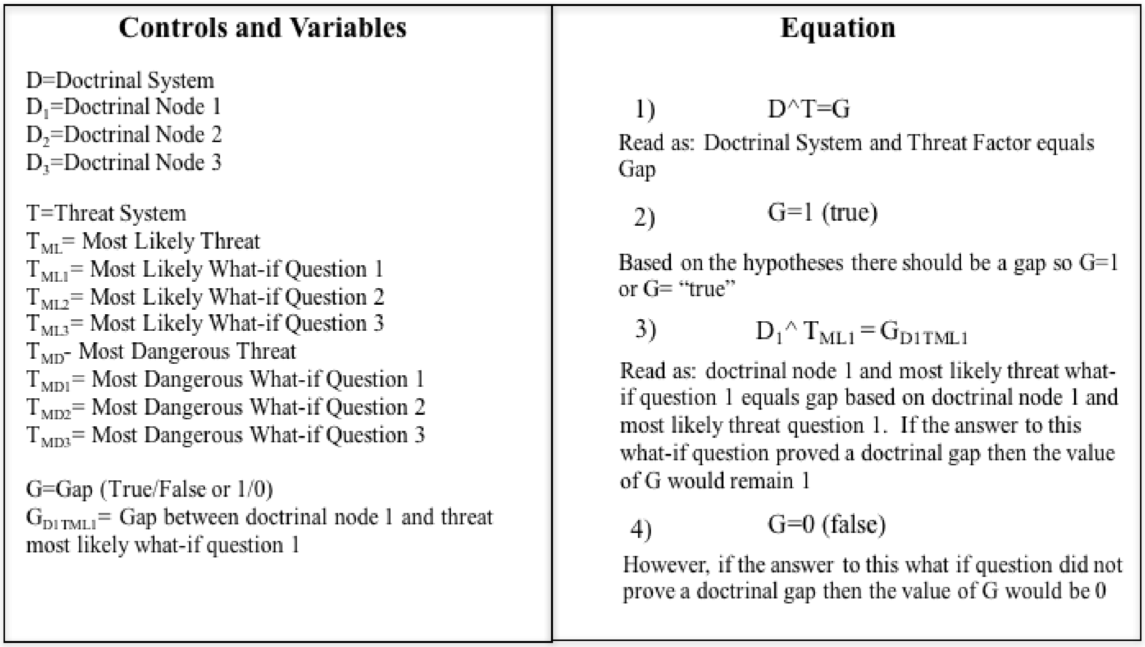
Logic Model

To assist running the experiments for both scenarios, I assigned variables to the systems and used a Boolean true or false equation to answer the what-if question. This allowed me to assign a binary numeric value to the outcome of each question supporting data collection, analysis, and interpretation.

For the doctrinal system, D= the entire modeled system, and D_1 = the first modeled doctrinal node. To limit the amount of iterations required achieve a solution, the experiments included only three doctrinal nodes, D_1 through D_3. Again, these nodes served as the control for both experiments.

For the threat system, T= threat, and T_{ML} = most likely threat while T_{MD} = most dangerous threat. Further, applying the three what-if questions per system developed six total variables to test the system. These what-if questions reflect as T_{ML1} through T_{ML3} and T_{MD1} through T_{MD3}.

As the hypotheses predicted there is a gap in doctrine, each logic question in the experiment resulted in and answer of either "true" or "false" in relation to that assertion. This enabled using the standard Boolean values of 0 for "false" and 1 for "true" Using G=gap, a "G" gap for each what-if question enabled a thorough analysis of the doctrinal system. The following figure reflects the derived equation along with controls and variables used in the experiments.



Controls and Variables

D=Doctrinal System
D_1=Doctrinal Node 1
D_2=Doctrinal Node 2
D_3=Doctrinal Node 3

T=Threat System
T_{ML}= Most Likely Threat
T_{ML1}= Most Likely What-if Question 1
T_{ML2}= Most Likely What-if Question 2
T_{ML3}= Most Likely What-if Question 3
T_{MD}- Most Dangerous Threat
T_{MD1}= Most Dangerous What-if Question 1
T_{MD2}= Most Dangerous What-if Question 2
T_{MD3}= Most Dangerous What-if Question 3

G=Gap (True/False or 1/0)
G_{D1TML1}= Gap between doctrinal node 1 and threat most likely what-if question 1

Equation

1) D^T=G

Read as: Doctrinal System and Threat Factor equals Gap

2) G=1 (true)

Based on the hypotheses there should be a gap so G=1 or G= "true"

3) D_1^ T_{ML1} = G_{D1TML1}

Read as: doctrinal node 1 and most likely threat what-if question 1 equals gap based on doctrinal node 1 and most likely threat question 1. If the answer to this what-if question proved a doctrinal gap then the value of G would remain 1

4) G=0 (false)

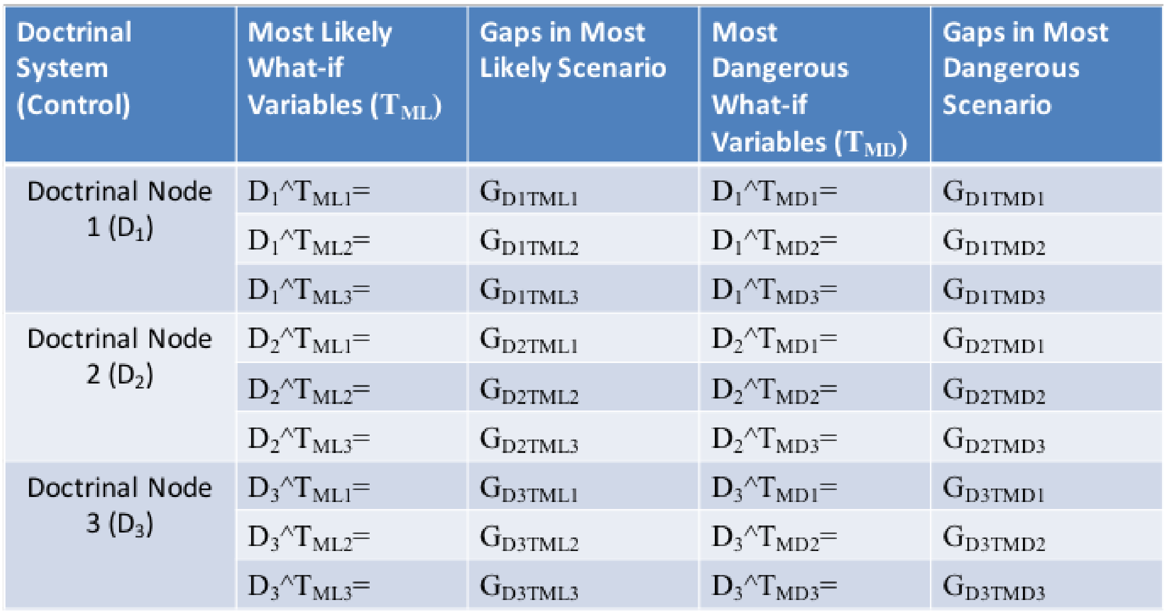
However, if the answer to this what if question did not prove a doctrinal gap then the value of G would be 0

Figure 3. Experiment Logic Equation, Controls and Variables

Source: Developed by author.

Asking all the what-if questions against all the doctrinal nodes provided 18 results in a "true" or "false" format supported by justification. These results directly answer secondary research question 3: if Army DSCA doctrine is no longer valid based on the most dangerous and most likely scenarios? As these "true" and "false" answers represent values of 1 and 0 respectively, I then evaluated that data. The following table graphically depicts the full range of questions as equations.

Table 1. Full Range of Questions as Equations



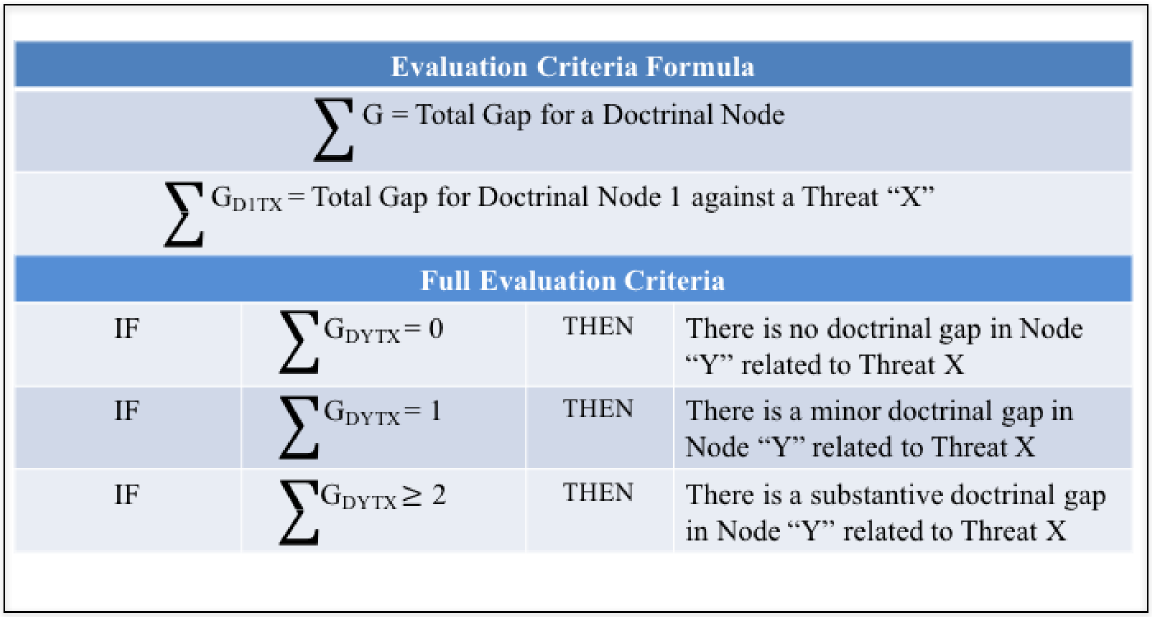
Doctrinal System (Control)	Most Likely What-if Variables (T_{ML})	Gaps in Most Likely Scenario	Most Dangerous What-if Variables (T_{MD})	Gaps in Most Dangerous Scenario
Doctrinal Node 1 (D_1)	D_1^T_{ML1}=	G_{D1TML1}	D_1^T_{MD1}=	G_{D1TMD1}
	D_1^T_{ML2}=	G_{D1TML2}	D_1^T_{MD2}=	G_{D1TMD2}
	D_1^T_{ML3}=	G_{D1TML3}	D_1^T_{MD3}=	G_{D1TMD3}
Doctrinal Node 2 (D_2)	D_2^T_{ML1}=	G_{D2TML1}	D_2^T_{MD1}=	G_{D2TMD1}
	D_2^T_{ML2}=	G_{D2TML2}	D_2^T_{MD2}=	G_{D2TMD2}
	D_2^T_{ML3}=	G_{D2TML3}	D_2^T_{MD3}=	G_{D2TMD3}
Doctrinal Node 3 (D_3)	D_3^T_{ML1}=	G_{D3TML1}	D_3^T_{MD1}=	G_{D3TMD1}
	D_3^T_{ML2}=	G_{D3TML2}	D_3^T_{MD2}=	G_{D3TMD2}
	D_3^T_{ML3}=	G_{D3TML3}	D_3^T_{MD3}=	G_{D3TMD3}

Source: Developed by author.

Evaluation Criteria

With numeric values associated with the true or false responses to the what-if questions, I then began analysis by applying the evaluation criteria. Since "G" gap yielded a value of 1 or 0 for each what-if question, aggregating the value of each "G" for a given doctrinal node provided the relative answer to how true the hypothesis remained. If the answer to each what-if question indicated that the doctrinal node remained valid, disconfirming the hypothesis, the value of G would be 0. By adding all the "G" scores for each doctrinal node in each scenario I established a scale of specifically how true the hypotheses remained after the test. If the sum of all "G" answers equaled 0, disconfirming the hypothesis, then no doctrinal gap existed. Likewise, if the sum of all "G" answers equaled 3, fully supporting the hypotheses, then a significant doctrinal gap existed. Using these extremes, I fully developed the criteria within the possible range of results. If the sum of "G" equaled 0 then no gaps existed. If the sum of "G" equaled 1, minor gaps existed as at least one what-if question supported the hypothesis. Finally, if the sum of "G" was greater than or equal to 2, then substantive gaps existed as most of the what-if questions supported the hypothesis. The following table depicts the evaluation criteria as well as examples.

Table 2. Evaluation Criteria and Examples



Evaluation Criteria Formula			
$\sum G$ = Total Gap for a Doctrinal Node			
$\sum G_{D1TX}$ = Total Gap for Doctrinal Node 1 against a Threat "X"			
Full Evaluation Criteria			
IF	$\sum G_{DYTX} = 0$	THEN	There is no doctrinal gap in Node "Y" related to Threat X
IF	$\sum G_{DYTX} = 1$	THEN	There is a minor doctrinal gap in Node "Y" related to Threat X
IF	$\sum G_{DYTX} \geq 2$	THEN	There is a substantive doctrinal gap in Node "Y" related to Threat X

Source: Developed by author.

Conclusion

The research methodology provided a framework to efficiently analyze a complex system like doctrine, and compare that system against a future threat. A routine methodology used in complex industrial processes and other disciplines such as medicine, SWIFT’s structured brainstorming helped to focus this study on key doctrinal principles, and tested them against realistic threat scenarios. The process began with selection of this methodology and led to the determination of five procedural steps to systematically answer the secondary research questions. The process controlled for bias by leveraging the research assumptions and integrating the hypothesis into two “experiments”.

Using the structured what-if questions to independently test each doctrinal node, I compared each node against the evaluation criteria. These criteria revealed both the existence of doctrinal gaps as well as a relative degree to which that gap exists. The degree to which a gap exists informed the analysis of the results.

The following chapter presents the data and analysis. Chapter four explains the selection of doctrinal nodes and outlines the determination of most likely and most dangerous scenarios. Additionally, the chapter explains the selection of what-if categories as well as the what if questions from both the most dangerous and most likely scenarios. The answers to those questions, as well as supporting justification, forms the basis for the answer to the primary research question, and sets a foundation for the conclusion.

CHAPTER 4

DATA PRESENTATION AND ANALYSIS

Introduction

This chapter builds directly from the previous chapter by adding specifics of the research problem into the research framework. This study utilized a modified what-if analysis called the structured what if technique or SWIFT. This chapter begins with restatement of the research question and continues with modeling of both the doctrine and the threat. The chapter concludes with the results from the SWIFT testing along with analysis of those results.

Hypothesis and Primary Research Question

Based on the problem statement outlined in chapter one, I developed a hypothesis that gaps exist in doctrine related to response during a cyber-attack. The primary research question is do gaps exist in Army DSCA doctrine that would jeopardize national interests during a cyber-attack on the homeland?

Secondary Research Questions

Breaking up the primary research question into several parts led to three secondary research questions. First, what does current Army doctrine say about responses during cyber-attacks on the nation? Answers to this question will help to model the DSCA system. Second, what are the most likely and most dangerous cyber-attacks scenarios? Answers to this question will help develop what-if questions to test the modeled DSCA system. Finally, what key parts of DSCA Doctrine are no longer valid based on the most dangerous and most likely scenarios.

SWIFT Process

As outlined in chapter three, the SWIFT process is an efficient and scalable methodology to identify gap and hazards in complex systems. I established a five-step framework based on this process integrating the hypothesis and secondary research questions into two "experiments" that identifies specific gaps related to aspects of a given threat. In the first step of this process I modeled the system. For this study that system included the key provisions of Army DSCA doctrine. I then modeled the threat to that system. Based on the literature review I determined a most dangerous and most likely scenario and established broad categories of those threats to structure brainstorming. Following the SWIFT protocol required development of what-if questions based on these structured categories. This resulted in a checklist that served as the threat model. Comparing the what-if questions against each of doctrinal provisions provided specific gaps. Integrating the hypothesis into the methodology allowed aggregation of those gaps and formed the basis for the evaluation criteria.

Doctrinal Context

The capstone Army Doctrine for Defense Support to Civil Authority is ADP 3-28, currently dated July of 2012. This manual provides the basic principles of DSCA for units executing DSCA from battalions to Army Service Component Commands (Department of the Army 2012, ii). ADP 3-28 defines DSCA as "federal military support for civil authorities in times of domestic emergencies for the purposes of saving lives, alleviating suffering, and protecting property" (Department of the Army 2012, iv). The next lower level of doctrine is the ADRP. For DSCA doctrine this is currently ADRP 3-28. This publication replaced FM 3-28, and provides a more in-depth discussion on

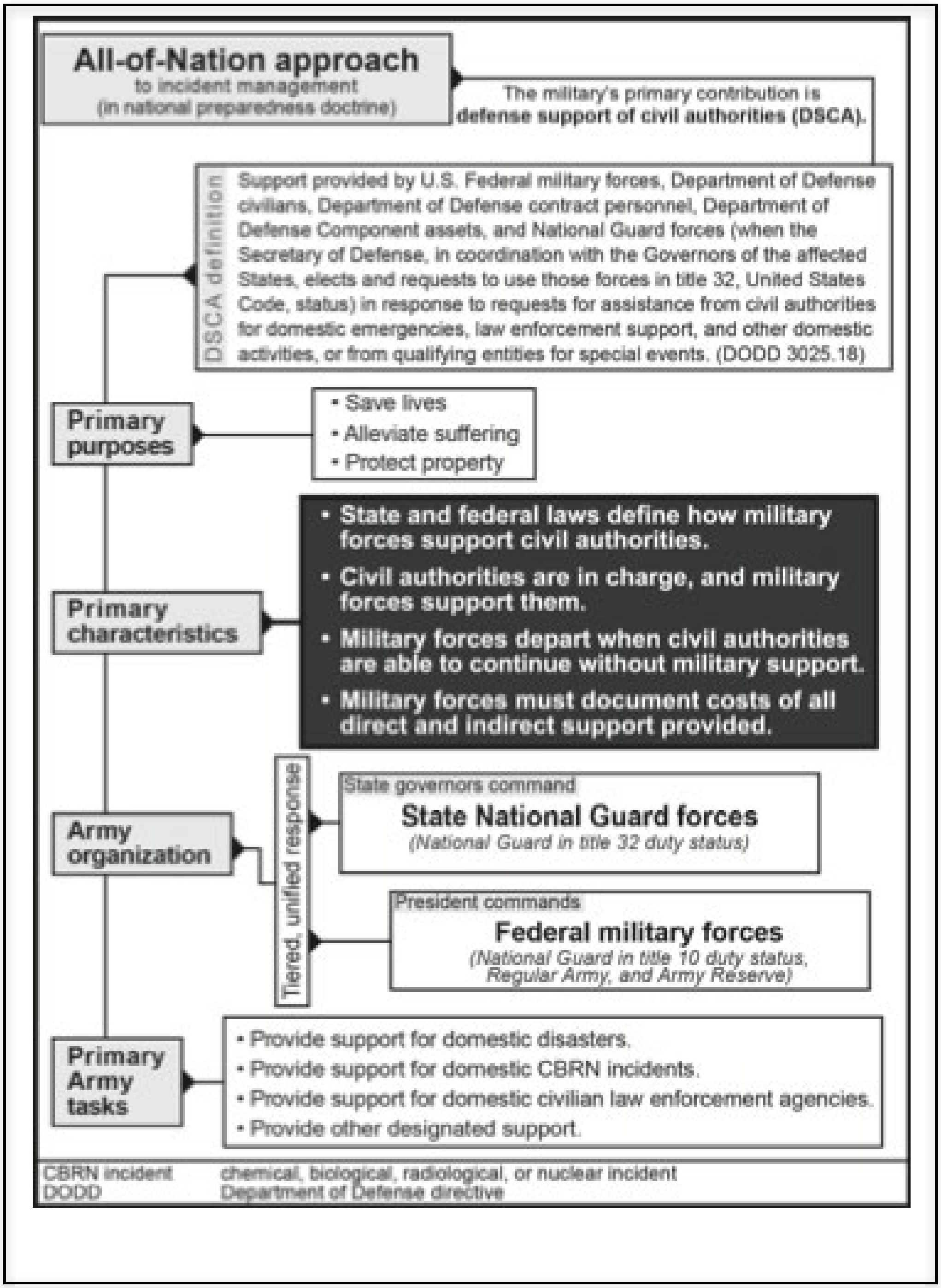
DSCA principles. This doctrine applies to all Active and Reserve Army units, referred to in DSCA doctrine commonly as Title 10 Forces, as well as federalized National Guard units. This doctrine nests with Joint Publication (JP) 3-28 which applies to the Joint Force including Joint Task Forces. One critical element in both Joint and Army doctrine includes the mutual exclusion of HD and DSCA. The critical element separating the two outlined in the doctrine is the authority as lead agency. In HD, the DoD leads, whereas in DSCA, an appointed civil authority leads (Department of Defense 2013b, vii). Finally, the Army utilizes ATP 3-28.1 dated February 2013 for specific "multi-service tactics techniques and procedure to plan, prepare, execute, and assess DSCA operations" (Air Land Sea Application Center 2013, i).

Though it is not DSCA doctrine, the most recently published Army doctrine, FM 3-0 *Operations*, includes two critical elements. First, FM 3-0 recognizes a significant increase in the threat environment as outlined in more recent national level strategy and policy documents. Part of this threat environment is enemy cyber-attacks against the homeland. Second, an operational manifestation of this threat is the inclusion of the defense industrial base and S-LOCs in the extended multi domain battlefield (Department of the Army 2017, 1-32).

Modeling Doctrine

Modeling the doctrine required two distinct actions to prepare a manageable control group of nodes that served as the Army DSCA doctrinal system. The first action reduced the doctrine from hundreds of pages of information into three critical nodes. The second action screened these nodes between all three major publications to ensure they accurately and universally represented the Army DSCA doctrinal system.

A starting point to reduce this system began with the Army definition of doctrine found in ADRP 1-02 as well as the purpose of doctrine found in ADP 1-01. In ADRP 1-02, the Army defines doctrine as the "fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application" (Department of the Army 2016b, 1-31). ADP 1-01 builds on ADRP 1-02 defining a "fundamental principle" as "comprehensive and fundamental rule or an assumption of central importance that guides how an organization or function approaches and thinks about the conduct of operations" (Department of the Army 2014a, 2-1). I used these definitions to screen the doctrine starting at the ADP level. ADP 3-28 contains a logic chart that serves as a full model of the Army's contribution to DSCA. As depicted in below figure, ADP 3-28 contains 13 ideas, or nodes, I considered fundamental principles.



All-of-Nation approach
to incident management
(in national preparedness doctrine)

The military's primary contribution is **defense support of civil authorities (DSCA).**

DSCA definition

Support provided by U.S. Federal military forces, Department of Defense civilians, Department of Defense contract personnel, Department of Defense Component assets, and National Guard forces (when the Secretary of Defense, in coordination with the Governors of the affected States, elects and requests to use those forces in title 32, United States Code, status) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events. (DODD 3025.18)

Primary purposes

- Save lives
- Alleviate suffering
- Protect property

Primary characteristics

- State and federal laws define how military forces support civil authorities.
- Civil authorities are in charge, and military forces support them.
- Military forces depart when civil authorities are able to continue without military support.
- Military forces must document costs of all direct and indirect support provided.

Army organization

Tiered, unified response

State governors command
State National Guard forces
(National Guard in title 32 duty status)

President commands
Federal military forces
(National Guard in title 10 duty status, Regular Army, and Army Reserve)

Primary Army tasks

- Provide support for domestic disasters.
- Provide support for domestic CBRN incidents.
- Provide support for domestic civilian law enforcement agencies.
- Provide other designated support.

CBRN incident	chemical, biological, radiological, or nuclear incident
DODD	Department of Defense directive

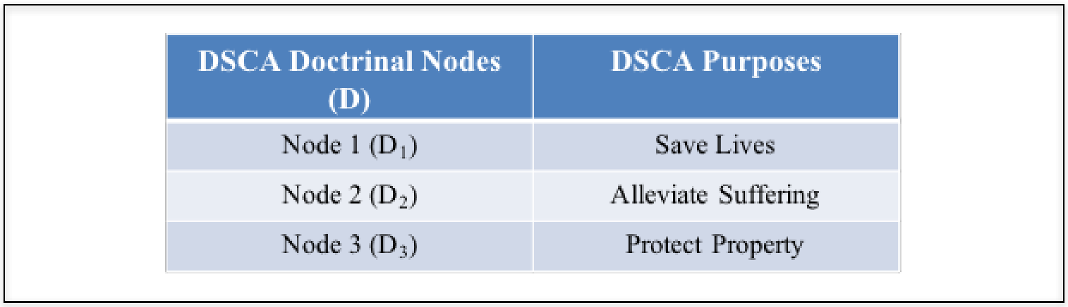
Figure 4. Overview of Defense Support to Civil Authority

Source: Department of the Army, Army Doctrine Publication 3-28, *Defense Support of Civil Authorities* (Washington, DC: Government Printing Office, July 2012), iv.

The publication groups these principles into four categories: purposes, characteristics, organization, and primary tasks. I used the ADP 1-01 key words of "fundamental rule or assumption," "central idea," and "guiding approach and thinking" to reducing these four categories into one. ADP 3-28 describes DSCA "primary purposes" as overarching, applicable to all DSCA missions, and the guidelines for action in the absence of orders (Department of the Army 2012, 5). Based on this analysis it was determined that the DSCA primary purposes of saving life, alleviating suffering, and protecting property serve a paramount importance. These purposes remain synonymous with principles per doctrinal definitions. These three purposes were selected as the three nodes to represent the doctrinal system.

After establishing the importance of these nodes, the next task included ensuring that these purposes reflect universal importance across the body of Army DSCA doctrine. A review of ADRP 3-28 and ATP 3-28.1 revealed that these three purposes remain of paramount importance throughout the entire body of Army DSCA doctrine. ADRP 3-28 begins chapter 2 with an explanation of these three core purposes, and retains their importance nearly verbatim from ADP 3-28. (Department of the Army 2013, 2-1). The techniques publication focuses on specific tactics regrading DSCA missions, but retains the importance of the three primary purposes when discussing authorities related to DSCA missions (Air Land Sea Application Center 2013, 3). Establishing the universal importance of the three DSCA purposes, the control group of nodes to test were established. The following table depicts the modeled doctrinal system.

Table 3. Modeled DSCA Doctrinal System



DSCA Doctrinal Nodes (D)	DSCA Purposes
Node 1 (D_1)	Save Lives
Node 2 (D_2)	Alleviate Suffering
Node 3 (D_3)	Protect Property

Source: Developed by author.

Fully answering the secondary research question required an additional step of investigating what the doctrine says about cyber-attacks. Using a document search function for the word "cyber", the word appeared only five times in all three doctrinal publications. Analysis showed the most significant mention of cyber-attack in ADRP 3-28 paragraph 2-22 which identifies the theoretical potential for a cyber-attack on the national power gird with cascading effects, creating a catastrophic event (Department of the Army 2013, 2-4). This mention, along with the other four incidences clearly validate the research assumption that DSCA doctrine would be used during a cyber-attack on domestic CIKR. Interestingly, ATP 3-28.1 does not contain any mention of cyber-attack despite containing an entire chapter on hazard specific guidance (Air Land Sea Application Center 2013, 81-101). Most significantly, ATP 3-28.1 defines protection of defense critical infrastructure from any external threat as a HD mission, separate from HS and DSCA. Further, ATP 3-28.1 states in chapter 1 that "missions are defined as homeland defense if the nation is under concerted attack (Air Land Sea Application Center 2013, 1). This definition remains closer to Joint Doctrine definitions for Defense

Critical Infrastructure Protection, but clearly conflicts with the cyber-attack scenario outlined in the ADRP.

Threat Context

As outlined in the relevant cyber theory section of the literature review, the two predominant schools of thought differ on current feasibility of cyber war, but do not preclude it as a future threat. Russia proved this capability in 2015 with a cyber-attack on Ukrainian power distribution network (NERC 2016, 1). In March of 2018, US-CERT, in conjunction with The Department of Homeland Security and the Federal Bureau of Investigation, published an advisory citing "a multi-stage intrusion campaign by Russian government cyber actors who targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks" (US-CERT 2018). This advisory also commented on intent stating "After obtaining access, the Russian government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems" (US-CERT 2018). As identified in the first chapter, this activity supports the assertion that actors possess the means, and remain prepared to act if given the motive and opportunity. With information gathered in the literature review, and recent threat reporting, I modeled the threat based on Russian APT activity targeting domestic CIKR.

Modeling Threat

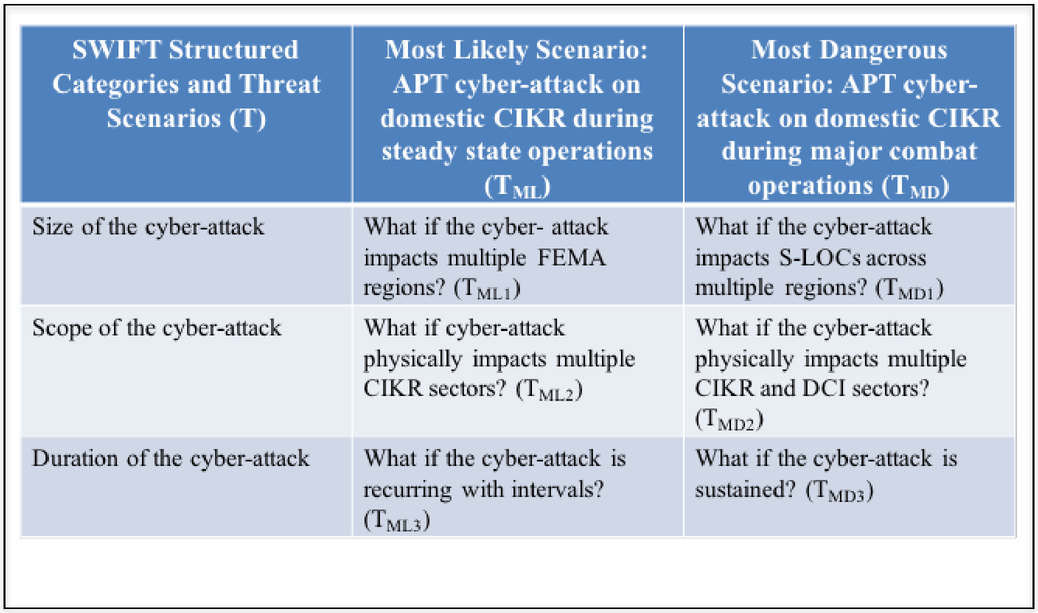
The first part of modeling the threat required separation of the threat into most likely and most dangerous scenarios. I defined most likely scenario as a cyber-attack targeting CIKR from an APT group without any major combat operations ongoing. In this scenario, the DoD would face steady state overseas operations while the bulk of the Active Duty Army, National Guard, and Army Reserve forces would be in the homeland in varying states of readiness. This scenario relied on the assumption that during an attack, cyber-defenses would fail at some point, and DSCA doctrine would be used to guide the response.

I defined the most dangerous scenario as a cyber-attack targeting CIKR from an APT group executed in conjunction with major overseas combat operations. In this scenario, the DoD would be in the process of deploying numerous Active Duty Army units, augmented by critical enablers from the Army Reserve, as well as units from the National Guard. This scenario relied on the assumption that adversaries will utilize cyber-attacks against domestic CIKR, cyber defenses will fail, and DSCA doctrine would still guide the response.

Following the structured what-if technique protocol, the next step required the development of broad categories to structure brainstorming of what-if questions. The logic I used to establish categories began with asking who, what, where, when, how, and why questions of each of the scenarios. For the purposes of this study I found the answers to who, why, and how either irrelevant or answered by assumptions. The remaining questions then established the broad categories for brainstorming. Category one became where the event could happen, or alternatively the relative size of the attack. Category two asked what was the nature of the attack, or alternatively the scale and scope of the attack. Finally, the third category asked when the attack would occur, refined to the duration of the attack.

The categories of size, scope, and duration structured brainstorming of what-if questions to continue SWIFT execution. Due to the limitations of this study I asked a single what-if question in each category, and from each scenario for a total of six questions. The following table depicts the six questions in each of their categories.

Table 4. Structured What-if Questions



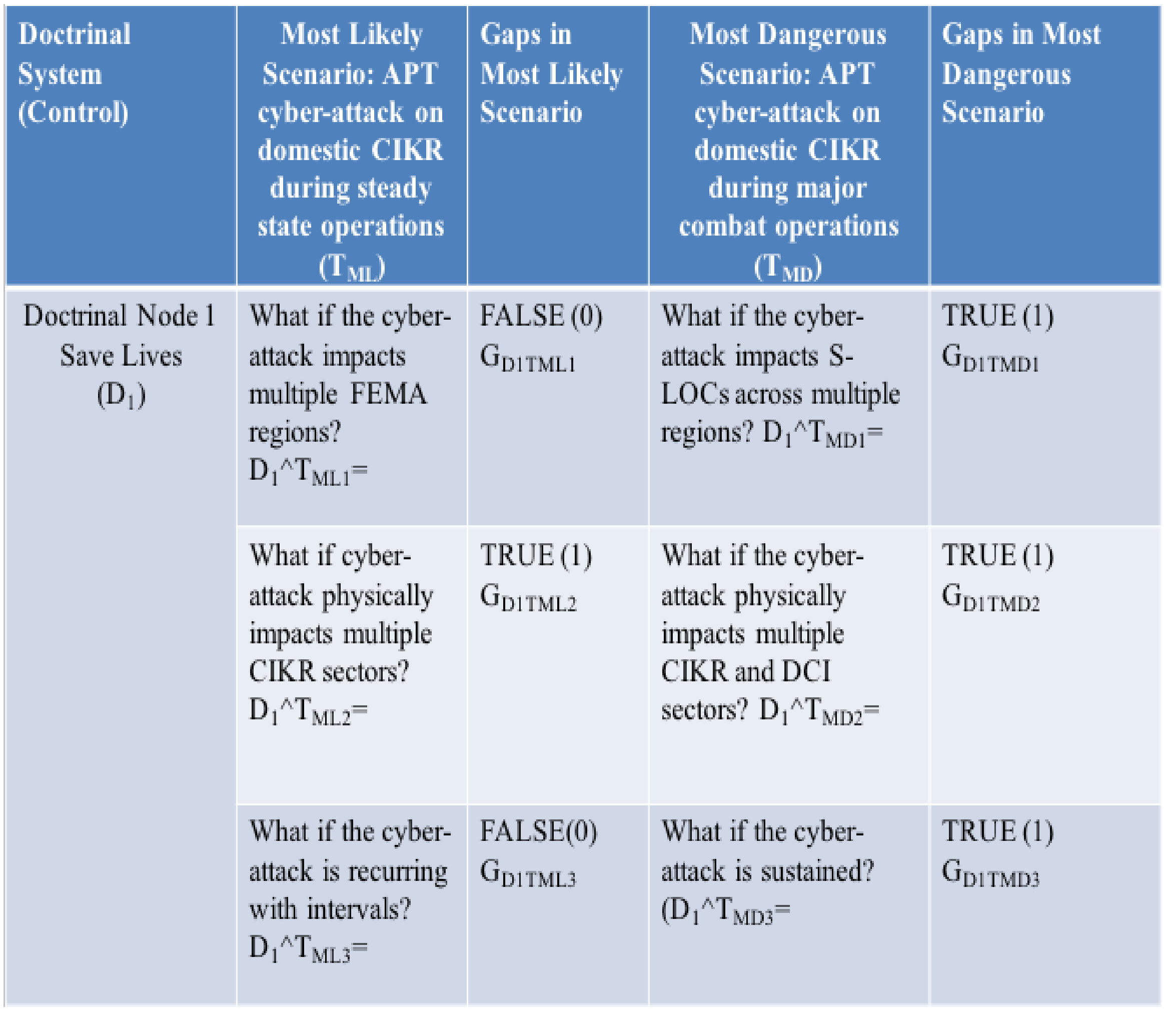
SWIFT Structured Categories and Threat Scenarios (T)	Most Likely Scenario: APT cyber-attack on domestic CIKR during steady state operations (T_{ML})	Most Dangerous Scenario: APT cyber-attack on domestic CIKR during major combat operations (T_{MD})
Size of the cyber-attack	What if the cyber- attack impacts multiple FEMA regions? (T_{ML1})	What if the cyber-attack impacts S-LOCs across multiple regions? (T_{MD1})
Scope of the cyber-attack	What if cyber-attack physically impacts multiple CIKR sectors? (T_{ML2})	What if the cyber-attack physically impacts multiple CIKR and DCI sectors? (T_{MD2})
Duration of the cyber-attack	What if the cyber-attack is recurring with intervals? (T_{ML3})	What if the cyber-attack is sustained? (T_{MD3})

Source: Developed by author.

SWIFT Experiments

Following the SWIFT protocol to determine gaps, experiments consisted of asking the three doctrinal nodes the six what-if questions. The full run of experiments yielded 18 results. The logic question for the first experiment preceded as: “True or false, the overarching DSCA purpose of saving lives is no longer valid if a cyber-attack impacts multiple Federal Emergency Management Agency (FEMA) regions. For this first experiment the answer of false disproved the hypothesis and indicated a gap did not exist. For the second experiment the logic question followed: “True of false, the overarching purpose of saving lives is no longer valid if a cyber-attack physically impacts multiple FEMA regions. For this second experiment, the answer of true supported the hypothesis and indicated a gap existed. The following three tables depict all 18 experimental results.

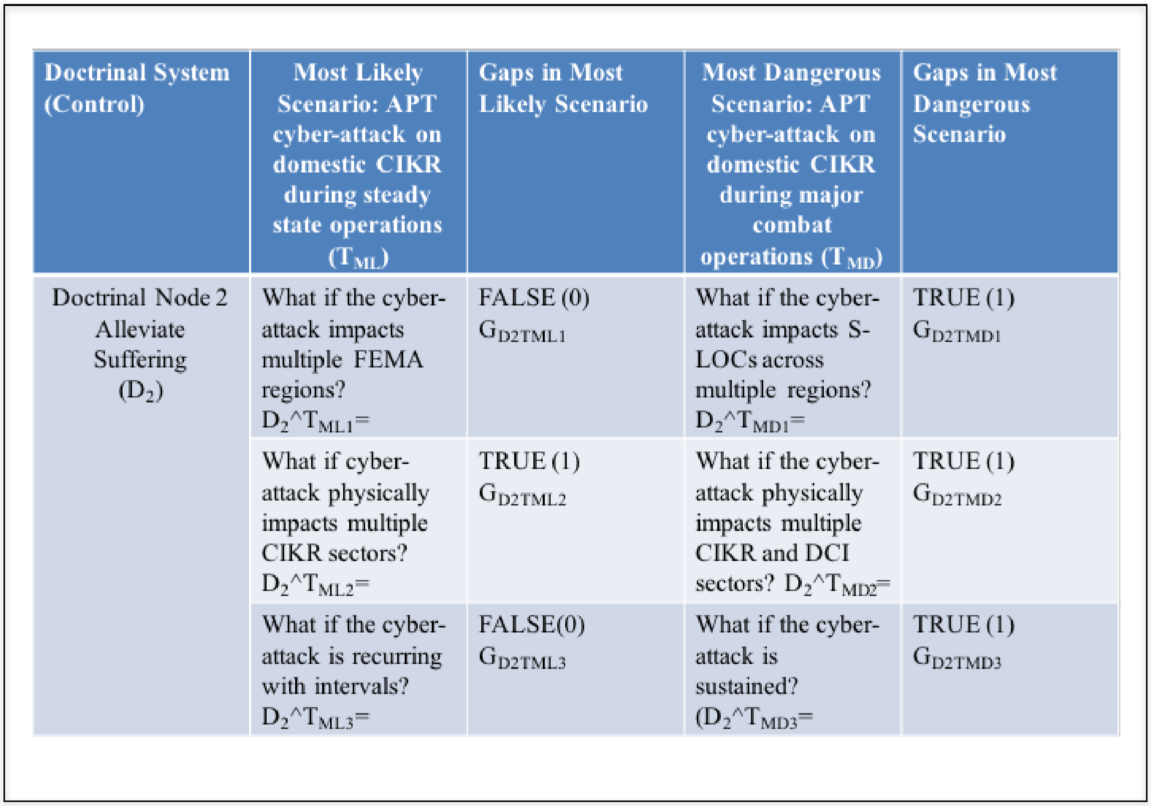
Table 5. Experimental Results for Doctrinal Node 1



Doctrinal System (Control)	Most Likely Scenario: APT cyber-attack on domestic CIKR during steady state operations (T_{ML})	Gaps in Most Likely Scenario	Most Dangerous Scenario: APT cyber-attack on domestic CIKR during major combat operations (T_{MD})	Gaps in Most Dangerous Scenario
Doctrinal Node 1 Save Lives (D_1)	What if the cyber-attack impacts multiple FEMA regions? D_1^T_{ML1}=	FALSE (0) G_{D1TML1}	What if the cyber-attack impacts S-LOCs across multiple regions? D_1^T_{MD1}=	TRUE (1) G_{D1TMD1}
	What if cyber-attack physically impacts multiple CIKR sectors? D_1^T_{ML2}=	TRUE (1) G_{D1TML2}	What if the cyber-attack physically impacts multiple CIKR and DCI sectors? D_1^T_{MD2}=	TRUE (1) G_{D1TMD2}
	What if the cyber-attack is recurring with intervals? D_1^T_{ML3}=	FALSE(0) G_{D1TML3}	What if the cyber-attack is sustained? (D_1^T_{MD3}=	TRUE (1) G_{D1TMD3}

Source: Developed by author.

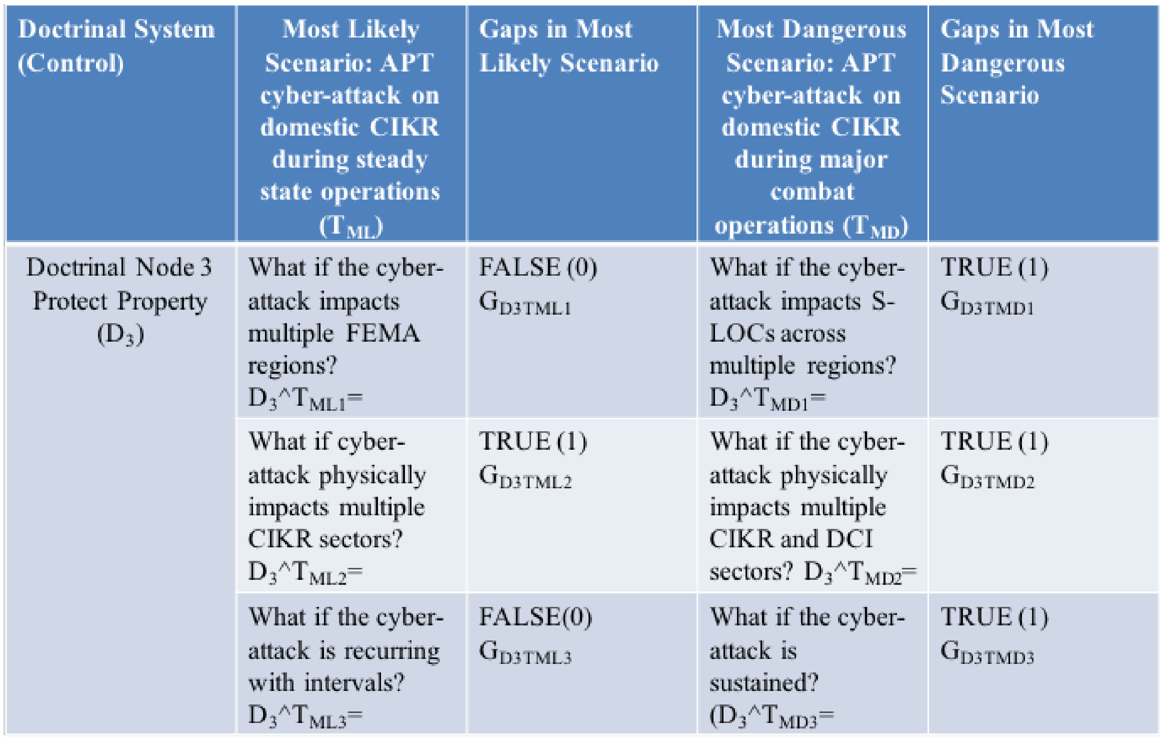
Table 6. Experimental Results for Doctrinal Node 2



Doctrinal System (Control)	Most Likely Scenario: APT cyber-attack on domestic CIKR during steady state operations (T_{ML})	Gaps in Most Likely Scenario	Most Dangerous Scenario: APT cyber-attack on domestic CIKR during major combat operations (T_{MD})	Gaps in Most Dangerous Scenario
Doctrinal Node 2 Alleviate Suffering (D_2)	What if the cyber-attack impacts multiple FEMA regions? D_2^T_{ML1}=	FALSE (0) G_{D2TML1}	What if the cyber-attack impacts S-LOCs across multiple regions? D_2^T_{MD1}=	TRUE (1) G_{D2TMD1}
	What if cyber-attack physically impacts multiple CIKR sectors? D_2^T_{ML2}=	TRUE (1) G_{D2TML2}	What if the cyber-attack physically impacts multiple CIKR and DCI sectors? D_2^T_{MD2}=	TRUE (1) G_{D2TMD2}
	What if the cyber-attack is recurring with intervals? D_2^T_{ML3}=	FALSE(0) G_{D2TML3}	What if the cyber-attack is sustained? (D_2^T_{MD3}=	TRUE (1) G_{D2TMD3}

Source: Developed by author.

Table 7. Experimental Results for Doctrinal Node 3



Doctrinal System (Control)	Most Likely Scenario: APT cyber-attack on domestic CIKR during steady state operations (T_{ML})	Gaps in Most Likely Scenario	Most Dangerous Scenario: APT cyber-attack on domestic CIKR during major combat operations (T_{MD})	Gaps in Most Dangerous Scenario
Doctrinal Node 3 Protect Property (D_3)	What if the cyber-attack impacts multiple FEMA regions? D_3^T_{ML1}=	FALSE (0) G_{D3TML1}	What if the cyber-attack impacts S-LOCs across multiple regions? D_3^T_{MD1}=	TRUE (1) G_{D3TMD1}
	What if cyber-attack physically impacts multiple CIKR sectors? D_3^T_{ML2}=	TRUE (1) G_{D3TML2}	What if the cyber-attack physically impacts multiple CIKR and DCI sectors? D_3^T_{MD2}=	TRUE (1) G_{D3TMD2}
	What if the cyber-attack is recurring with intervals? D_3^T_{ML3}=	FALSE(0) G_{D3TML3}	What if the cyber-attack is sustained? (D_3^T_{MD3}=	TRUE (1) G_{D3TMD3}

Source: Developed by author.

Justification

Running all 18 experiments yielded three out of nine cases, under the most likely scenario, where the hypothesis remained true, and nine out of nine cases, under the most dangerous scenario, where the hypothesis remained true. Under the most likely scenario all three responses of true returned for the question: what if the cyber-attack physically impacts multiple CIKR sectors. Successful attacks across multiple CIKR sectors would create cascading effects and become catastrophic event across the entire homeland. In this scenario, the majority of Active Duty Army, National Guard, and Army Reserve forces would be available to the DoD and lead disaster coordinating agency. However, successful attacks across the energy, transportation, utilities, and communication CIKR sectors would create a currently unmanageable problem for the Army. Part of the problem in this scenario involves the supply and demand for response assets. With several CIKR sectors impacted, and long term physical damage possible, Army DSCA support would be prioritized first to the most critical sectors. High demand Army capabilities, such as emergency power generation, engineering, transportation, and aviation would be dedicated to restoring services before any other tasking. Further, the cascading nature of the attack would put the Federal Government into a Continuity of Government (COG) situation at the same time as demand for support at state and local levels would continue to escalate. Again, in this situation, the Army DSCA enterprise would need to restore essential services to itself and the federal government before all other priorities. This challenges the assertion that in all situations the purpose of the Army is to save lives, alleviate suffering, and protect property.

Under the most dangerous scenario, all nine responses of true returned indicating that all three what-if questions indicated gaps exist. Similar to the most likely scenario, these gaps involve prioritization and resource allocation. During a major overseas combat operation, where the enemy employs a cyber-attack on domestic and defense CIKR, the Army's number one priority will be continuity of operations to support the Geographic Combatant Commander. In this situation, the same capabilities required by state and local governments would be required by the combatant commanders on top of those requirements from the federal government. Faced with both a continuity of government and continuity of operations problem there would be no Army component capable of responding as part of a tiered response. The best use for the Army in this situation would be terminating the source of the cyber-attack through decisive action. Additional factors in this situation include the demand on strategic lift, global logistics, and supplies. In this situation, the purpose of DSCA would be continuity of operations and government universally over all other priorities.

Analysis

Using the evaluation criteria on the data produced several results. First, all three doctrinal purposes received a score of "1" in the most likely scenario indicating minor gaps in doctrine. Second all three doctrinal purposes received a score of "3" in the most dangerous scenario indicating substantive gaps in doctrine. The category of "scope" returned all true responses indicating that cyber-attacks impacting multiple CIKR sectors in either scenario pose the greatest gap in doctrine. Finally, the differential between scores of "3" and "9" for the most likely and most dangerous scenarios respectively indicates problems with the flexibility of the doctrine to adequately respond to the current range of threats.

Conclusion

Following the SWIFT process provided logical and sequential answers to all research questions within the limitations of the study. This process started with building a model for Army DSCA doctrine which resulted in three doctrinal nodes corresponding to each primary purpose for DSCA. This process also answered the first secondary research question. After modeling the doctrine, the next step involved modeling the threat by establishing most dangerous and most likely scenarios, and developing structured what-if scenario based questions to test the doctrine. This process answered the second secondary research question. Comparing the results of the what-if questions to the evaluation finalized provided data for analysis and interpretation and answered the third research question.

Doctrinal gaps exist in Army DSCA doctrine jeopardizing national interests during a cyber-attack on the homeland related to the core purpose of DSCA in catastrophic event attacks impacting multiple CIKR sectors, and during the execution of major combat operations.

The following chapter reiterates the SWIFT analysis, findings, and interpretation of the results. Additionally, this final chapter makes doctrinal recommendations and recommendations for future study.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Introduction

This research project started with the identification of a problem related to both current and emerging threats. In the multi-domain battle concept, the homeland is no longer a secure strategic base of operations to project force from. With the homeland now part of the extended battlefield in the cyber domain, the nation must face some new realities. Threat reporting indicates the initial moves preparing cyber-attacks from our adversaries remain ongoing (US-CERT 2018). This research sought to investigate this new threat and determine if it changed the doctrine guiding the Army's response in the homeland.

Identification of the problem led to a hypothesis that gaps exist in doctrine related to response during a cyber-attack on the homeland. The primary research question became: do gaps exist in Army DSCA doctrine that would jeopardize national interests during a cyber-attack on the homeland? Breaking up the primary research question into several parts led to three secondary research questions. First, what does current Army doctrine say about responses during cyber-attacks on the nation? Answers to this question will helped to model the DSCA system. Second, what are the most likely and most dangerous cyber-attacks scenarios? Answers to this question will helped develop what-if questions to test the modeled DSCA system. Finally, are parts of DSCA Doctrine are no longer valid based on the most dangerous and most likely scenarios

This chapter presents the findings to those questions along with interpretation of those results. Following the interpretation of the results, this chapter offers recommendations based on the study. Finally, this chapter lays out some areas for future study related to the problem.

Findings

Using the Structured What-if Technique to answer the research questions, the study produced the following results:

1. Minor gaps exist in the core purposes outlined in Army DSCA doctrine relating to cyber-attacks against multiple CIKR sectors.
2. Substantive gaps exist in the core purposes outlined in Army DSCA doctrine relating to cyber-attacks during the simultaneous execution of major combat operations
3. Army DSCA doctrine lacks flexibility to address the complex and potentially catastrophic impact of cyber-attacks on CIKR.

Interpretation

Interpreting these results led to several key observations. First is a dilemma between COG/COO and traditional DSCA. Both responses require contribution from the Army to a civil authority. In COG or COO situations the Army provides support to the federal government to keep the mechanisms of government functioning in a national emergency. In DSCA the Army supports a civil authority as part of a tiered response to any level of emergency. However, based on the analysis of the first finding, these two requirements to support different civil authority may exist simultaneously. Given limited critical resources, a clear line must be drawn for catastrophic events where COG is the priority of the nation. This entails new purposes, tasks, organization, and characteristics that may look very different from DSCA doctrine.

Second, despite the requirement to support civil authorities under the NRF, the entire structure of DSCA doctrine breaks down when integrating future large-scale combat operations against capable adversaries. I believe this is due in part to DHS control over the NRF, and based largely on the responses to Hurricane Katrina and the 9-11 terror attacks. This framework works well when mutually excluding the execution of a major combat operation overseas. Aspects of this problem include the lack of both federal and state resources specifically the Army Reserve and significant capabilities from the National Guard, and well as simultaneous problems sets of COG, COO and DSCA. Looking at this problem from the other perspective, Unified Land Operations definitively sets DSCA as mutually exclusive from major combat operations. The graphical depiction of decisive action shows a combination of offense defense and stability while overseas and draws a literal line separating DSCA from these tasks. This may need to look more like the simultaneous execution of offense, defense, stability, and DSCA in support of Unified Action.

Finally, the threats facing the nation, now and in the future, continue to blur the lines between DSCA and HD. A cyber-attack from a peer adversary may not bear the signature of a nuclear strike on the nation, but the impact may be just as catastrophic. DSCA doctrine does not remain flexible to these threats. Again, there is a mutual exclusion between DSCA and HD that does not reflect reality. Today there is more of a range of military operations in the homeland that incorporates everything from support for DSCA type wildland firefighting through HD type catastrophic COO and COG events.

Recommendations

Based on the results of this study I recommend several doctrinal changes. First, Army DSCA doctrine should be updated by integrating the extended multi domain battlefield as outlined in FM 3-0. This extended battlefield, combined with current threats, alter two doctrinal "lines" that previously existed. First, the "line" separating operations in the United States from operations overseas no longer exists in the extended battlefield. Second, the "line" between DSCA and HD is blurred at best based on threats from cyberspace. Analysis of the logic chart in ARDP 3-0 describing the Army's operational concept clearly shows the problem with these lines. The following figure depicts the lines as they appear with remarks.

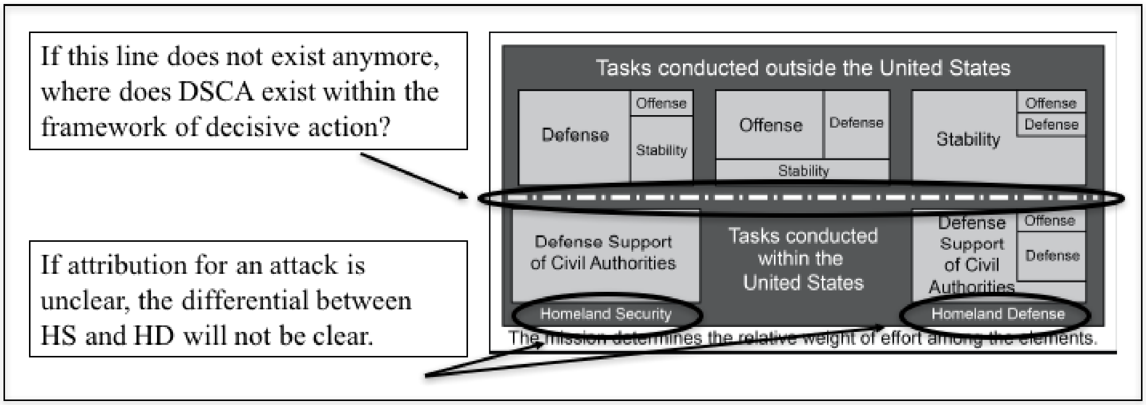
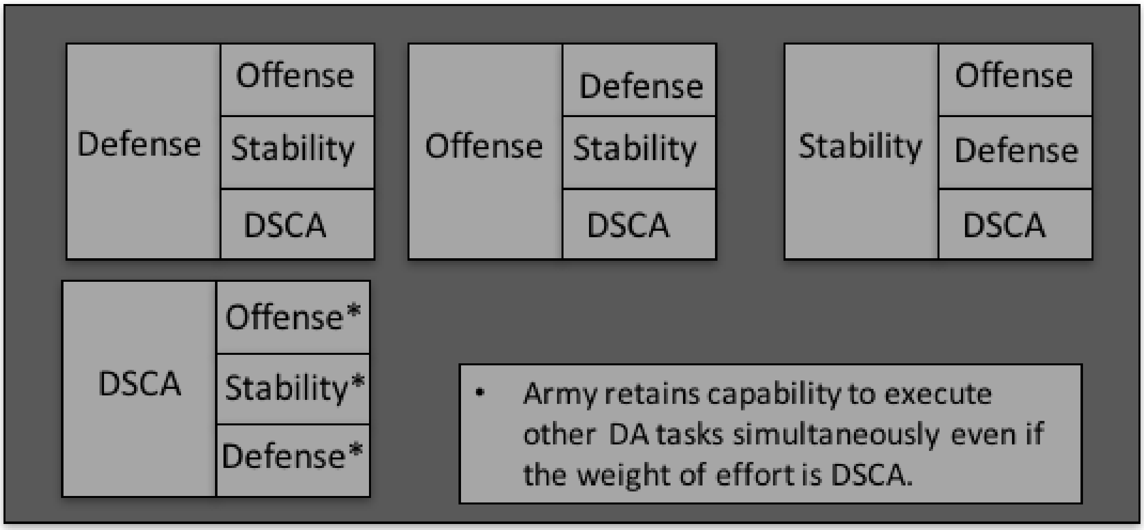

If this line does not exist anymore, where does DSCA exist within the framework of decisive action?
If attribution for an attack is unclear, the differential between HS and HD will not be clear.
Tasks conducted outside the United States
Defense
Offense
Stability
Offense
Defense
Stability
Stability
Offense
Defense
Defense Support of Civil Authorities
Tasks conducted within the United States
Defense Support of Civil Authorities
Offense
Defense
Homeland Security
Homeland Defense
The mission determines the relative weight of effort among the elements.

Figure 5. Comments on Decisive Action

Source: Department of the Army, Army Doctrine Reference Publication 3-0, *Operations* (Washington, DC: Government Printing Office, 2016), 3-3.

As depicted above, cyber-attacks remain ungoverned by geography and bring the possibility of simultaneous operations overseas and in the homeland. If the decisive action therefore must account for the simultaneous execution of offense, defense, stability, and DSCA. The following figure serves as a representation of decisive action that accounts for a multi domain extended battlefield.



- Army retains capability to execute other DA tasks simultaneously even if the weight of effort is DSCA.

Figure 6. Recommended Decisive Action Framework

Source: Developed by author.

Based on the blurring of the line between DSCA and HD, doctrine must provide more flexibility. Difficulty discerning the origin of a cyber-attack will have consequences for lead agency selection, authorities, and prioritization of effort. If an adversary executes a cyber-attack in concert with other military operations, national authorities will begin far behind the enemy's decision cycle. Army doctrine must account for this new challenge and should provide flexibility through a range of operations along a continuum. DSCA and HD should evolve into *Operations in the Homeland*, placed on a Range of Military Operations in the Homeland, and should incorporate COG and Operations at the high end of the spectrum of conflict. The following figure depicts a recommended spectrum to view these *Operations in the Homeland.*

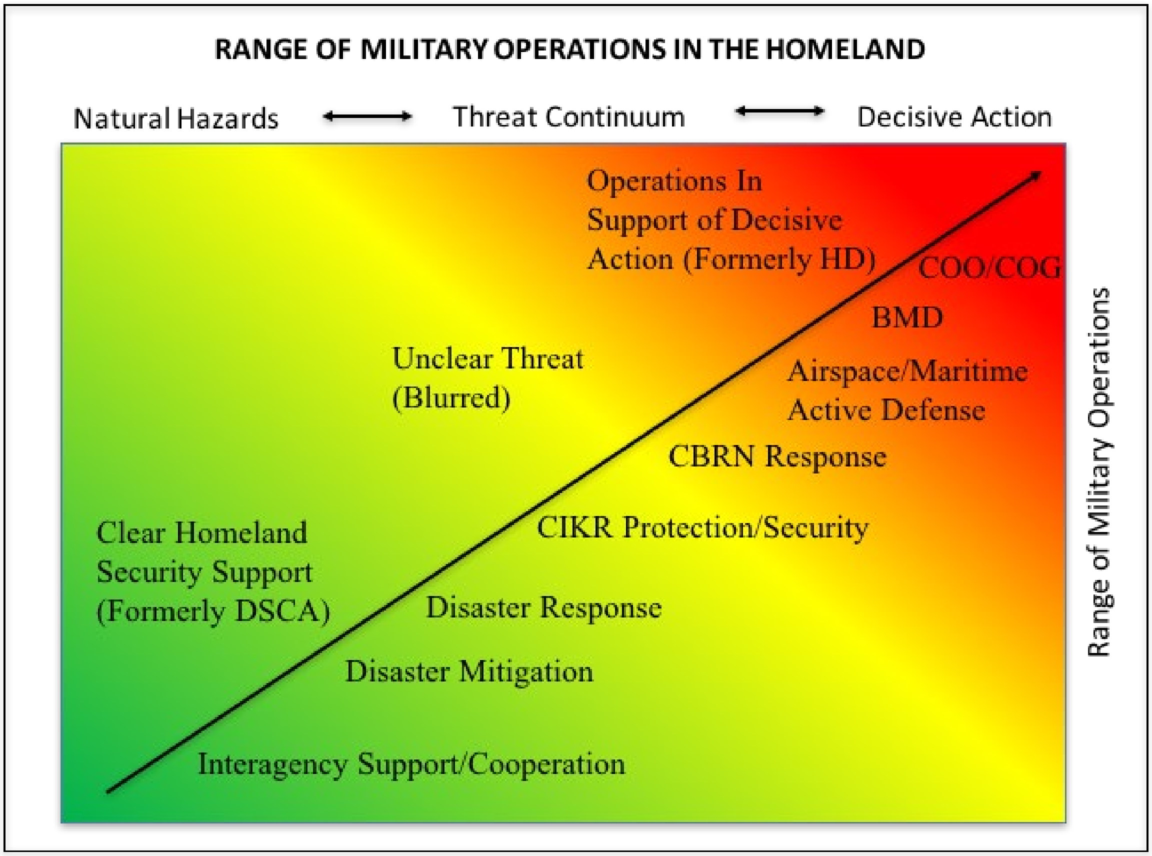

RANGE OF MILITARY OPERATIONS IN THE HOMELAND
Natural Hazards
Threat Continuum
Decisive Action
Operations In Support of Decisive Action (Formerly HD)
COO/COG
BMD
Airspace/Maritime Active Defense
CBRN Response
Unclear Threat (Blurred)
CIKR Protection/Security
Clear Homeland Security Support (Formerly DSCA)
Disaster Response
Disaster Mitigation
Interagency Support/Cooperation
Range of Military Operations

Figure 7. Recommended Range of Operations in the Homeland

Source: Developed by author, based on Department of the Army, Army Field Manual 3-0, *Operations* (Washington, DC: Government Printing Office, 2017), 1-1.

Future Study

Areas of future study regrading this problem should focus on what to do next, challenge other paradigms, and seek ways to apply these lessons across the enterprise. The next logical step for this problem is to begin to reshape DSCA doctrine. This thesis identified gaps in the current doctrine. Following studies must conduct a capability based assessment to identify doctrinal needs. This may begin with a concept for operations in the homeland. Given the nature of the cyber threat, this study should include USNORTHCOM and integrate joint and interagency partners.

With gaps identified in the fundamental purposes of DSCA, what other gaps exist based on this threat? The Joint Publications should be studied as well as the NRF to answer this question. Outside of DSCA related doctrine, proponents should reframe their traditional problems based on multi domain battle as determine if gaps exist in their respective doctrines.

Finally, in addition to doctrinal updates, other DOTMLPF-P capabilities will be required to address this threat. Studies on the most efficient ways to do this should follow capabilities based assessments. An example of this would be in the areas of organization, training, and material what capability is required to achieve an enterprise response supporting the Cyber National Mission Forces?

The impact of Hurricane Katrina drove the last major changes to DSCA doctrine. From that event, the nation established the NRF, and National Incident Management System which informed DoD doctrine. In the period of time before the next multi domain war, it is essential for the nation to reframe the problem and adjust accordingly.

Final Thoughts

Taking the *cyber* out of this entire study and replacing it with *space* or *electromagnetic* would not greatly alter the results. The critical fact remains that the homeland is now vulnerable to attack from a variety of adversaries with dangerous weapons. The civilian population is no longer safe, the homeland is no longer a safe strategic base, critical infrastructure will be attacked, and force projection will become increasingly difficult. Despite this alarmist tone, this is the reality of a world where the United States cannot achieve superiority in every domain. The emergence of multi domain battle is the forerunner to a new and dangerous environment that presents unprecedented threats to our national interests. The nation must begin to study and adapt to this environment, or suffer the consequences of inaction.

REFERENCE LIST

Acquisition Safety and Environmental Management System. 2017. “SWIFT.” Last updated 28 November. Accessed 1 April 2018. https://www.asems.mod.uk/ toolkit/swift.

Air Land Sea Application Center. 2013. ATP 3-28.1, MCWP 3.26.2, NTTP 3.57.2, AFTTP 3.2.67, *Multi-Service Tactics, Techniques, and Procedures for Defense Support of Civil Authorities and Integrating with National Guard Civil Support*. Washington, DC: Government Printing Office.

American Chemical Society. 2016. “What-if Analysis.” Last updated 14 July. Accessed 1 April 2018. https://www.acs.org/content/acs/en/about/governance/committees /chemicalsafety/hazard-assessment/ways-to-conduct-hazard-assessment/what-if-analysis.html.

Army National Guard. 2017. *Vision and Strategy*. Arlington, VA: Army National Guard. Accessed 3 January 2018. http://www.nationalguard.mil/Portals/31/ Documents/ARNGpdfs/2017-arng-vision-strategy-02272016.pdf.

Boyd, Bradley L. 2009. “Cyber Warfare: Armageddon in a Teacup?” Master’s Thesis, U.S. Army Command and General Staff College, Fort Leavenworth, KS.

Chairman, Joint Chiefs of Staff. 2015. *The National Military Strategy of the United States.* Washington, DC: Government Printing Office. Accessed 22 December 2017. http://www.jcs.mil/Portals/36/Documents/Publications/2015_ National_Military_Strategy.pdf.

Chekinov, S. G., and S. A. Bogdanov. 2013. “The Nature and Content of a New-Generation War.” *Journal of Military Thought*, no. 4: 12-23. Accessed 12 April 2018. http://www.eastviewpress.com/Files/MT_FROM%20THE %20CURRENT%20ISSUE_No.4_2013.pdf.

Connell, Michael, and Sarah Vogler. 2017. *Russia’s Approach to Cyber Warfare*. Arlington, VA: CNA Analysis and Solutions. Accessed 10 February 2018. https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

Department of the Army. 2012. Army Doctrine Publication (ADP) 3-28, *Defense Support of Civil Authorities*. Washington, DC: Government Printing Office.

———. 2013. Army Doctrine Reference Publication (ADRP) 3-28, *Defense Support of Civil Authorities*. Washington, DC: Government Printing Office.

———. 2014a. Army Doctrine Publication (ADP) 1-01, *Doctrine Primer*. Washington, DC: Government Printing Office.

———. 2014b. *Army Strategic Planning Guidance*. Accessed 23 November 2017. http://www.g8.army.mil/pdf/Army_Strategic_Planning_Guidance2014.pdf.

———. 2016a. Army Doctrine Reference Publication (ADRP) 3-0, *Operations*. Washington, DC: Government Printing Office.

———. 2016b. Army Doctrine Reference (ADP) Publication 1-02, *Terms and Military Symbols*. Washington, DC: Government Printing Office.

———. 2016c. *Doctrine Smart Book*. Washington, DC: Government Printing Office.

———. 2017. Army Field Manual (FM) 3-0, *Operations*. Washington, DC: Government Printing Office.

Department of Defense. 2013a. Joint Publication 3-27, *Homeland Defense*. Washington, DC: Government Printing Office.

———. 2013b. Joint Publication 3-28, *Defense Support to Civil Authorities*. Washington, DC: Government Printing Office.

———. 2015. *The Department of Defense Cyber Strategy*. Washington, DC: Government Printing Office.

———. 2016. "All Cyber Mission Force Teams Achieve Initial Operating Capability." U.S. Cyber Command News Release, 24 October. Accessed 3 November 2017. https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/.

———. 2018. *National Defense Strategy Summary*. Washington, DC: Government Printing Office. Accessed 11 February 2018. https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Department of Homeland Security. 2006. *Cyber Storm: Exercise Report*. Washington, DC: Homeland Security. Accessed 3 October 2017. https://www.dhs.gov/sites/default/files/publications/Cyber%20Storm%20I%20After%20Action%20Final%20Report.pdf.

———. 2009. "CIKR." Accessed 3 April 2018. https://www.dhs.gov/blog/2009/11/19/cikr.

———. 2016. *Cyber Storm V: After Action Report*. Washington, DC: Homeland Security. Accessed 3 October 2017. https://www.dhs.gov/sites/default/files/publications/CyberStormV_AfterActionReport_2016vFinal-%20508%20Compliant%20v2.pdf.

Electricity Information Sharing and Analysis Center. 2016. *Analysis of the Russian Attack on the Ukrainian Power Grid*. Washington, DC: Electricity Information Sharing and Analysis Center. Accessed 12 December 2017. https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38, no. 2 (Fall): 41-73.

Government Accountability Office. 2016. GAO-16-332, *Civil Support, DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents*. Washington, DC: Government Accountability Office. Accessed 12 December 2017. https://www.gao.gov/products/GAO-16-332.

Government Publishing Office. 2016. *Blackout! Are We Prepared to Manage the Aftermath of a Cyberattack or Other Failure of the Electrical Grid?* Accessed 12 December 2017. https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg99931/pdf/CHRG-114hhrg99931.pdf.

Hopes, Christopher A. 2013. "The Challenges of Defense Support to Civil Authorities and Homeland Defense in the Cyber Domain." White Paper, Naval War College, Newport, RI.

Kirkland, Kristian J. 2008. "The Army National Guard; Operational Reserve or Homeland Security Force?" Master's Thesis, U.S. Army Command and General Staff College, Fort Leavenworth, KS.

Larson, Eric V., and John E. Peters. 2001. *Preparing the U.S. Army for Homeland Security, Concepts, Issues, and Options*. Santa Monica, CA: Rand Corporation. Accessed 14 February 2018. http://www.jstor.org/stable/10.7249/mr1251a.14.

Libicki, M. 2015. "The Cyberwar that Wasn't." In *Cyber War in Perspective: Russian Aggression against Ukraine*, edited by Kenneth Geers, 49-54. Tallinn, Estoria: NATO Cyber Center of Excellence.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: Rand Corporation. Accessed 20 April 2018. https://www.rand.org/pubs/monographs/MG877.html.

Muniz Jr., Jorge. 2009. "Declawing the Dragon: Why the U.S. Must Counter Chinese Cyber-Warriors." Master's Thesis, U.S. Army Command and General Staff College, Fort Leavenworth, KS.

Nakasone, LTG Paul M., and MAJ Charlie Lewis. 2017. "Cyber Space in Multi-Domain Battle." *The Cyber Defense Review* 2, no. 3 (March): 15-24. Accessed 15 March 2018. http://cyberdefensereview.army.mil/The-Journal/Article-Display/Article/1134630/cyberspace-in-multi-domain-battle/.

National Guard Bureau. 2016. CNGBM 3510.01, *National Guard Homeland Response Force and Chemical, Biological, Radiological, Nuclear, and High Yield Explosive Enhanced Response Force Package Procedures*. Arlington, VA: National Guard Bureau, August 2016. Accessed 14 January 2018. http://www.ngbpdc.ngb.army.mil/pubs/CNGBI/CNGBM3510_01_20160925.pdf.

North American Electric Reliability Corporation (NERC). 2012. *2011 NERC Grid Security Exercise: After Action Report*. Washington, DC: North American Electric Reliability Corporation. Accessed 12 December 2017. https://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC_GridEx_AAR_16Mar2012_Final.pdf.

———. 2016. *Grid Security Exercise: GridEx III Report*. Atlanta, GA: North American Electric Reliability Corporation. Accessed 12 December 2017. https://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf.

Singer, P. W., and Allaw Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press.

Symantec. 2017. "Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group." *Symantec Blogs*, 20 March. Accessed 15 January 2018. https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks.

U.S. Army Reserves. 2017. *The Army Reserve Posture Statement*. Accessed 22 February 2018. http://www.usar.army.mil/About-Us/Posture-Statement/.

United States Computer Emergency Readiness Team (US-CERT). 2017. Alert (TA17-293A), *Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors*. Accessed 1 November 2017. https://www.us-cert.gov/ncas/alerts/TA17-293A.

———. 2018. Alert (TA18-074A), *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.* Accessed 29 March 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A.

U.S. President. 2017. *The National Security Strategy of the United States of America*. Washington, DC: The White House. Accessed 12 February 2018. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

Valeriano, Brandon, and Ryan C. Maness. 2014. "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-11." *Journal of Peace Research* 51, no. 3 (April): 347-360.