WWW.KASSERINEPASS.COM: DETERMINING THE U.S. ARMY'S READINESS FOR TACTICAL OPERATIONS IN CYBERSPACE.

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
General Studies

by

André Bernard Abadie, MAJ, USA
B.S. Computer Engineering, United States Military Academy, West Point, NY, 1996
M.S. Information Assurance, University of Maryland University College, Adelphi, MD, 2008

Fort Leavenworth, Kansas
2009

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
12-06-2009	Master's Thesis	AUG 2008 – JUN 2009

4. TITLE AND SUBTITLE
WWW.KASSERINEPASS.COM: Determining the U.S. Army's Readiness for Tactical Operations in Cyberspace.

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

André Bernard Abadie

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

The dominance of the U.S. Army's conventional capabilities has forced our adversaries to generate asymmetric techniques in order to marginalize our advantages. One technique they may pursue is to target our extensive use of information technology. The reliance our commanders place on the benefits of cyberspace, combined with the massive proliferation of hostile cyber tactics, suggests our tactical units are destined to face such a threat. When considering the consequences of not addressing this risk, lessons learned from the Battle of Kasserine Pass resonate. Though history provides numerous examples of units entering battle unprepared, Kasserine Pass is unique in that it was preceded by the innovation of a major combat capability; the tank and armored warfare. A tactical disaster, Kasserine Pass highlighted the vulnerability of the force during the critical time between an innovation's implementation and its institutionalization. The new concepts must be incorporated into doctrine, organizations, training, leader development, and materiel in order for Soldiers to utilize them on the battlefield. For those at Kasserine Pass, institutionalizing the innovation that eventually won the war came too late.

15. SUBJECT TERMS
Cyber Warfare, Network Warfare, Electronic Warfare, Information Warfare, Innovation

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)	80	

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 André Bernard Abadie

Thesis Title: WWW.KASSERINEPASS.COM: Determining the U.S. Army's Readiness for Tactical Operations in Cyberspace.

Approved by:

_____, Thesis Committee Chair
Jack D. Kem, Ph.D.

_____, Member
LTC John E. Bircher, IV, M.A.

_____, Member
Brian G. Blew, M.S.

Accepted this 12th day of June 2009 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

WWW.KASSERINEPASS.COM: DETERMINING THE U.S. ARMY'S READINESS FOR TACTICAL OPERATIONS IN CYBERSPACE, by MAJ André Bernard Abadie, 80 pages.

The dominance of the U.S. Army's conventional capabilities has forced our adversaries to generate asymmetric techniques in order to marginalize our advantages. One technique they may pursue is to target our extensive use of information technology. The reliance our commanders place on the benefits of cyberspace, combined with the massive proliferation of hostile cyber tactics, suggests our tactical units are destined to face such a threat. When considering the consequences of not addressing this risk, lessons learned from the Battle of Kasserine Pass resonate. Though history provides numerous examples of units entering battle unprepared, Kasserine Pass is unique in that it was preceded by the innovation of a major combat capability; the tank and armored warfare. A tactical disaster, Kasserine Pass highlighted the vulnerability of the force during the critical time between an innovation's implementation and its institutionalization. The new concepts must be incorporated into doctrine, organizations, training, leader development, and materiel in order for Soldiers to utilize them on the battlefield. For those at Kasserine Pass, institutionalizing the innovation that eventually won the war came too late.

ACKNOWLEDGMENTS

This thesis was my opportunity to apply previous graduate studies in Information Assurance to my professional duties (the military environment). It would not have been initiated if not for the immediate and continuous support from my wife, Linda. Additionally, the benefit of this research and analysis effort was significantly enhanced by the support and dedication of my committee.

Dr. Jack Kem is the Command and General Staff College's Distinguished Chair for Innovation and a Supervisory Professor. When writing a paper analyzing the criticality of institutionalizing innovation in today's operational environment, there can be no better Committee Chair. Dr. Kem is a retired Military Intelligence Colonel with extensive experience in support of Airborne operations and the tactical level of war. LTC John "Chip" Bircher has just departed the U.S. Army Computer Network Operations and Electronic Warfare Proponent (USACEWP) within the Combined Arms Center. As the Deputy Director (Futures) he was the optimum selection for 2nd Reader as a subject matter expert in this emerging field. LTC Bircher has transitioned to USCENTCOM as an IO Planner. Mr. Brian Blew is a Tactics Instructor at the Command and General Staff College. Having exhausted the last year teaching me tactics, he knows me best and has the mission of keeping my focus on the tactical level of war and our modular force while making a concerted effort to prevent my writing style from entering 'geekdom.' Mr. Blew is a retired aviator with extensive experience at the brigade level.

Finally, LTC Harry Friberg--my first Signal boss and enduring mentor--instilled in me a desire for self-development in the technical competencies that dominate our role as Signal Officers. This is a continuation of my quest for such knowledge.

TABLE OF CONTENTS

Page

ACRONYMS

ABCS	Army Battle Command Systems
AFATDS	Advanced Field Artillery Tactical Data System
AMDWS	Air and Missile Defense Workstation
ASAS	All-source Analysis System
BCS3	Battle Command Sustainment and Support System
C2DS	Command and Control (C2) Data System
CA	Civil Affairs
COCOM	Combatant Command
COP	Common Operational Picture
CPOF	Command Post of the Future
CSSCS	Combat Service Support Control System
CTIS	Combat Terrain Information System
FBCB2	Force XXI Battle Command Brigade and Below
GIG	Global Information Grid
IMETS	Integrated Meteorological System
IO	Information Operations
MCS	Maneuver Control System
NETCOM	Network Enterprise Technology Command
NIPRNET	NONSECURE Internet Protocol Router Network
PAO	Public Affairs Officer
PSYOP	Psychological Operations
SIPRNET	SECRET Internet Protocol Router Network
TAIS	Tactical Airspace Integration System

ILLUSTRATIONS

Page

CHAPTER 1

INTRODUCTION

> The tank battalion chosen to lead the counterblow had never seen combat.
> "Off we went across the desert," a lieutenant recalled.
> "We knew not what we were getting into."
> It is pardonable to be defeated . . . but unpardonable to be surprised.
> — Rick Atkinson, *An Army at Dawn (2002)*

> Every age has its own kind of war, its own limiting conditions and its own peculiar preconceptions.
> — Carl von Clausewitz, *On War (1832)*

The Inherent Risk in Innovation

Innovation is a fickle endeavor. Born of creativity and vision, it has to be adopted by a vocal proponent capable of effectively communicating its benefits. It must be sold to a political bureaucracy in order to gain approval for implementation and introduction to the force. And though implementation brings a taste of success, it is just a way-point along the path towards institutionalization. In order to be accepted, the innovation must be developed in concert with the doctrine, training, and organizational frameworks of its customers. Once synchronized to best complement existing and established activities, it can demonstrate its value to the force. It is in this effort towards institutionalization that there is evidence of significant risk. Though the lack of an innovation may place the force at a disadvantage to a technically superior foe, the presence of an immature innovation presents confusion, error, and mistakes. With regard to cyber warfare, the U.S. Army is currently in this period and history warns that it is in jeopardy. Is there a looming Battle for Kasserine Pass in the future of cyberspace- a potential www.kasserinepass.com?

The Battle of Kasserine Pass

In November 1942, Operation Torch introduced American troops into combat on the Atlantic side of World War II. Since the initial resistance of landings was by the French- who were not the enemy- the actual first major battle against Germany and the Axis powers did not occur until January 1943, when enemy efforts to secure a series of mountain passes developed into the Battle of Kasserine Pass. This first battle between American and German forces would signify the preparedness of the U.S. Army's tactical units for contemporary warfare. Having witnessed the Germans' introduction of armored warfare in such a dominant fashion, the leaders who spent over a decade trying to innovate our own force with similar capabilities would unfortunately recognize the validity of their argument first-hand. Some of the most significant lessons of the interwar period can be drawn from observations during the Battle of Kasserine Pass. "Organizations and men were still largely in tune with the time and space factors that had prevailed in the previous war. They had yet to adjust to the accelerated tempo and increased distances of the battlefield- in particular, the necessary speed of reaction so well understood by their adversaries" (Blumenson 1986, 240). When the battle concluded, German losses totaled 200 men killed, 550 wounded, and 250 missing; 20 tanks, 6 half-tracks, 61 motor vehicles, and 14 guns destroyed. American losses totaled 300 men killed, 3,000 wounded, and 3,000 missing; 183 tanks, 104 half-tracks, 512 motor vehicles, and 208 guns destroyed. In short, the Battle of Kasserine Pass was a disaster for the U.S. Army (Blumenson 1986, 260).

"The Americans made many mistakes in this first large-scale engagement of the war in Europe, but they learned from their errors and made adjustments that enabled them

to go on to victory in Tunisia and beyond. The defeat at Kasserine showed the Army what troops had to learn and to do" (Blumenson 1986, 265). The lessons derived from Kasserine Pass were not just based on experiences of that battle, but also of mistakes or misdirection during the interwar period. Kasserine Pass "reflected the strategic assumptions and other intellectual baggage, training and doctrine that the U.S. Army carried into World War II" (Heller and Stoft 1986, xi). If one lesson rang true it was the acceptance of mechanization as a reality of warfare and the birth of an American armored force. A closer review of that development allows us to recognize the transition from the despair at Kasserine Pass to the dominance of Patton's Third Army.

An in-depth study of the actual events at Kasserine Pass to support this thesis is unnecessary. The intent of this study is to argue against reliving the incident in cyberspace. Rather, examining some of the details in how the U.S. Army proceeded from the fall of 1939 (the German sweep through Poland) until the fall of 1942 (U.S. executes Operation Torch) can guide what the U.S. Army should do now to avoid a similar tragedy in cyberspace. The fall of 1939 clarified the existence of a new threat and the fall of 1942 was the initial deployment to engage this threat. It was during this time period that the U.S. Army assessed itself as unprepared for that current threat and the contemporary battle space- and thus created the Armor branch in order to innovate the force. The successes of Patton's Third Army indicate it was the right decision. However, the premature utilization of armored warfare by the soldiers at Kasserine Pass highlights the criticality of expediting the institutionalization of innovations.

Armored Warfare

As the year 1939 concluded the United States Army kept a cautious eye on foreign nations demonstrating the power of armored warfare against their adversaries; carefully exploring its potential while discerning confusing terminology and negotiating the intra-service battles between branches regarding its proper role amongst the force. This interest was not new as the idea of mechanization emerged at the end of World War I; however, budgetary constraints had kept military developments at a minimum.

The entrance of armored warfare, like most new concepts, entailed some initial confusion regarding terminology. "Motorization" described the use of motor vehicles, typically those used outside of combat. This description was more an essence of the current technology vice any innovation, as the motorized vehicle was becoming more standard throughout developed nations. On the contrary, "mechanization" was often used as the descriptive for armored, tracked combat vehicles. "Motorization was often seen as an easier, cheaper, less revolutionary change than mechanization" (House 1984, 45). Finally the term "tank" was used to depict any form of armored vehicle or mechanized unit, not only an armored, tracked, turreted, gun-carrying fighting vehicle. Such a broad application of the term made it difficult "to determine if a speaker was discussing pure tank forces, mechanized combined arms forces, or mechanization of infantry forces" (House 1984, 45). When the Army later created a separate Armored Force, "the name 'Armor' was chosen for the new force in order to avoid using the terms 'Mechanized,' which had been used by the cavalry, or 'Tank,' which had been used by the infantry" (Bielakowski 2002, 41).

The little experimentation that had occurred following the first World War ceased in 1932 when Army Chief of Staff Douglas MacArthur disbanded the experimental force and directed all mechanized assets placed under the Cavalry. MacArthur made his decision based on the belief that "the cavalry was the traditional arm of mobility and maneuver and that made it the natural place for mechanized forces" (Bielakowski 2002, 28). Throughout the next decade numerous training exercises would test various concepts for the role of the mechanized force; however, emergence of the 'combat arm of decision' was still in wait. In actuality, "the cavalry and infantry branches continued to view mechanization as only an auxiliary to their existing forces, rather than as a revolutionary weapon" (Bielakowski 2002, 40). Their opposing views reached a culmination in June 1940 when Army Chief of Staff George C. Marshall assembled a meeting to discuss the future role of mechanized forces. The conference ended without a consolidated recommendation or any formal decision because "the branch chiefs argued for control of the development of mechanized forces" (House 1984, 45). Within weeks, Marshall created the separate Armored Force. There was no time to wait for the branches to resolve their differences, the Army was not prepared for the warfare being demonstrated across the Atlantic and it needed to start addressing its shortfalls.

In 1938, Germany attacked Austria then Czechoslovakia. As the world watched, they attacked Poland in September of 1939. In the spring of 1940, the Germans launched an offensive into Holland and Belgium. Within days they were pushing into France and by June 22, 1940 the French had all but completely surrendered. In less than two years, Germany had successfully defeated Czechoslovakia, Poland, Holland, Belgium, and now France. The defeat of France, which had previously made progress towards the

development of a mechanized force, only reinforced the dire consequences which lay ahead for the Americans. “French armoured divisions lacked the doctrine, training, communications, and above all the conception of combined arms to handle the complex and fluid environment within which the Germans fought. As a result the French fought as individuals rather than as units and the resulting discrepancy between the opposing forces was all too obvious” (Murray 1995, 309). The U.S. Army’s creation of a separate Armored Force came just days after the French surrender. The time it would take to incorporate the concepts into doctrine, organizations, training, leader development, and personnel would be tenuous with a clear enemy present. Armor had been born, but not tested nor proven. Kasserine Pass would come first.

Cyber Warfare

As the year 2008 concluded the U.S. Army kept a cautious eye on foreign nations demonstrating the power of cyber warfare against their adversaries; carefully exploring its potential while discerning confusing terminology and negotiating the intra-service battles between branches regarding its proper role amongst the force. The operational targeting of a government’s information infrastructure prosecuted through electronic forms of attack against their computer networks and systems is not exactly revolutionary. It is a well established criminal activity used by our adversaries being redirected as a pursuit of a different “end.” The “ways” and “means” have been witnessed for the last decade in the form of cyber crime against the U.S. Government.

As with any new concept, there are varying definitions in use to specify exactly what is being pursued. For example, “digitization” describes the use of computers to automate a system or process. It has relevance in all aspects of the military, whether it be

combat or administrative. Like motorization before it, digitization is more a representation of the current technological environment. Everything from cars to refrigerators are being digitized in today's developed nations. "Networking" is an advancement that allows computers or specific digitized systems to share data. Typically referred to as "net-centric" within the Army, to be networked is a more advanced level of technology than digitization and provides a greater capability to the force. It is similar to mechanization being an enhancement to a motorized vehicle; networking allows a digitized system to share its data. "Electronic warfare" is used to define attack, protect, or support functions using the electromagnetic spectrum. Such a broad application of the term makes it difficult to determine if the speaker is discussing pure electronic warfare via radio wave propagation or network warfare utilizing cyberspace. To be completely understood, the purpose (attack, protect, support) and medium (radio, cyber) must be articulated.

Like all other emerging topics within the Army, cyberspace as a domain has produced parochialism amongst the functional branches and a continued debate regarding who is best postured to fill this operational void. The Military Intelligence community made the initial grab for cyber warfare since it is a logical subset of electronic warfare. Since its inception, electronic warfare has been an Intelligence responsibility, so this was as logical as mechanization's subordination to Cavalry. However, cyber warfare is in itself a computer-based activity. When the Army embraced the computer as an enabler of the force, the Signal Corps assumed the responsibility of integrating them into organizations. This support relationship is rooted in time, just as the consistent support role mechanization brought to the Infantry community during its development. Finally,

the Artillery has entered the discussion based on their assumed role as the proponent for effects. Cyber warfare will be an activity directed against an enemy, and therefore it will provide an effect. Currently, the effects community has placed cyber warfare as an aspect of Information Operations. Who is best postured to lead the necessary development of cyber warfare at the tactical level? Is there ambiguity in its current execution based on the varied approaches by each branch proponent?

In 2003, a series of Chinese cyber attacks against the United States was labeled *Titan Rain* (Norton-Taylor 2007, 3). Though precise origins of the attack, as well as the exact methods of the attack, have not been disclosed, it provided the international community with the first portrayal of a cyber attack from a nation-state. In 2007, the government of Estonia was crippled by assumed Russian cyber attacks (Marsan 2007, 22). More importantly, this attack gave the first glimpse of cyber being used to impart a military effect as it resembled the cyber version of a military air campaign. Shortly thereafter in 2008, similar actions took place in the country of Georgia. Of specific interest, the actions against Georgia occurred in concert with military operations against the country. If the world questioned the previous events and their purpose, Georgia erased all doubt and demonstrated a valid signature of cyber warfare.

The Department of Defense (DoD) has steadily migrated towards operations in cyberspace and the recognition that the environment will influence the future- in terms of both general warfare and national security. What is not abundantly clear is whether or not the Army has acknowledged this entity at any level below the strategic level of war. Is there not an expectation that tactical units, the centerpiece of our modular Army, are going to be expected to prosecute their influence within cyberspace? In 1995, Forces

Command and the Training and Doctrine Command began a joint venture called Force XXI with the objective to ensure the superiority of our command and control system by providing warfighters with a horizontally and vertically integrated digital network. "Task Force XXI (TFXXI) and Division XXI Advanced Warfighter Experiments (AWE) were the capstone events of this venture. . . . At the heart of this experiment was near real-time location knowledge of friendly units down to individual vehicles, and in some cases, individual soldiers" (Metz et al. 2006, 3). The creation of this tactical internet was successfully validated by recent operations, specifically Operation Iraqi Freedom. Leveraging its applications internally for command and control purposes is but one innovation institutionalized by the military to enhance our prosecution of warfare.

The question remains as to whether the Army has innovated its digital capabilities to fully utilize the Internet and the existing global network as a mechanism for a commander to prosecute his influence upon the greater battlespace. The U.S. Army created a tactical network (with Internet technologies) and applied it to the tactical level. Recent operational experience has demonstrated this effort has been institutionalized. What happens when that tactical internet connects to the global Internet and places our formation in space? What is its potential innovation as a form of warfare or weaponry once exercised within the global domain? There is published doctrine for operations within air, land, and sea as well as tactics, techniques, and procedures for those elements of our contemporary operational environment. However, cyberspace remains an uncertainty and the U.S. Army may find itself challenged by tomorrow's digital battle for www.kassinepass.com. Therefore, this study will be focused on the Army's tactical force and the ability of modular units to operate within cyberspace.

Primary Research Question

The purpose of this thesis is to study the readiness of the Army's tactical force to conduct cyber warfare. To reach a determination, the focus will be to recognize the Brigade Combat Team and Division's ability to operate in cyberspace and its role as the modular Army prosecutes cyber warfare. The primary research question asks, "Is the Army ready for cyber warfare at the tactical level of operations?"

Secondary Research Question

There are two secondary research questions that shape the answer to the primary research question. First, is there a cyber requirement at the tactical level? Prior to dissecting the Brigade Combat Team and Division's posture with regard to cyberspace, an understanding of the domain must be fully understood. This requires recognition of the systems and networks used by the U.S. Army to execute tactical operations. Additionally, it requires an understanding of how those systems and networks tie into the greater Internet or global networks. A comprehensive understanding of the cyberspace environment will clarify the tactical reach into operational and strategic levels based on the capabilities of existing technologies. Finally, the numerous adversaries that abound within cyberspace and constitute the threat need to be reviewed and applied with concern towards any possible accessibility they may have to a Brigade Combat Team or Division's networks. Recognizing the significance of the cyber environment and threats with regard to the Army's modular force will set the context for the criticality of their preparation.

Second, has the U.S. Army prepared Divisions and Brigade Combat Teams for the execution of cyber warfare? The expectation of the U.S. Army is that it prepares for

the operations it will conduct. The priority or likelihood of their conduct generally explains the variance in an organization's ability to perform specific missions. The previous question will set the reader's expectation for how prepared the Division and Brigade Combat Team needs to be to operate in cyberspace. This question will be analyzed using the standard method of DOTMLPF criteria. DOTMLPF reviews doctrine, organization, training, leader development, materiel, personnel, and facilities to best summarize the overall status of an organization. More importantly, it examines functional criteria the Army is responsible to provision. The study does not target the unit training records, rather it scrutinizes the training personnel receive from the Army's institutions in order to prepare for assignment to a Division or Brigade Combat Team. Each criteria takes the same approach to ensure the scrutiny is placed at the Army level, not the tactical unit.

Significance

The dominance of the United States Army's conventional capabilities has forced our adversaries to generate asymmetric techniques in order to marginalize our advantages. An additional technique they may pursue is to target our extensive use of information technology. The reliance our Commanders place on the benefits of cyberspace, combined with the massive proliferation of hostile cyber tactics, suggests this domain will emerge and confront our units in the future. As stated in the 2008 National Defense Strategy, "the predominant near-term challenges to the United States will come from state and non-state actors using irregular and catastrophic capabilities. Although our advanced space and cyber-space assets give us unparalleled advantages on the traditional battlefield, they also entail vulnerabilities" (Gates 2008, 22). This paper will explore

those potential vulnerabilities at the tactical level and assess the readiness to face these near-term challenges.

Assumptions

This study assumes that adequate information exists at the unclassified level. It further presumes that all unclassified information will be available for review and analysis. This is of particular importance for staff actions awaiting decision, those currently being deliberated prior their approval, or those pending official release.

Limitations & Delimitations

This is an unclassified study using unclassified sources dated prior to 19 January 2009. This study focuses on the Brigade Combat Team with reference to the Division as an immediate higher headquarters. It does not explore cyber warfare above the tactical level.

This chapter suggested a historical analogy to depict the significance of this research topic, while providing a basic understanding of the subject as it relates to the current operational environment. The next chapter relates to the research question by detailing the various literature researched in order to answer the question. It will identify what is and is not known already. It will present the literature analyzed with respect to the aforementioned research questions. The primary question will be broken down by the two secondary questions, and those secondary questions further detailed by tertiary questions.

CHAPTER 2

LITERATURE REVIEW

> Although our research has inherent limitations (for example we rely exclusively on published sources), we trust that publication of our findings will serve as a primer on cyber warfare matters, accessible to expert and nonprofessional alike.
>
> — Charles Billo and Welton Chang, *Cyber Warfare (2004)*

> I've not found much at all explicitly linking cyber war with the BCT or the tactical level of war. . . . I'll be glad to try further, but for now I'm stymied.
>
> — Research Technician, *Combined Arms Research Library (2008)*

The primary research question of this study asks this, "Is the Army ready for cyber warfare at the tactical level of operations?" This chapter relates to the research question by detailing the various literature researched in order to answer the question. It will identify what is and is not known already. The previous chapter suggested a historical analogy to depict the significance of this research topic, while providing a basic understanding of the subject as it relates to a contemporary operational environment. This chapter will present the literature analyzed with respect to the questions it addressed. The primary question was broken down by the two secondary questions, and those secondary questions further detailed by tertiary questions.

Cyberspace as a domain is emerging, as well as the concept of cyber warfare as an operational practice. The preponderance of literature that specifically addresses military networks and capabilities originates from the Army War College at Carlisle Barracks, though it is admittedly descriptive of the strategic environment. Most literature focusing on cyberspace within the commercial sector addresses cyber warfare as cyber terrorism. This literature allows insight into adversarial tactics and methodology- crime is merely

warfare waged by non-state actors. As an example, *Brave New War: The Next Stage of Terrorism and the End of Globalization* by John Robb has been well received by the security community and provides a broad review of the future enemy and threat environment- with the exception that it is articulated as a tactical attack with strategic effects. Robb states that "the rise of superempowered groups is part of a larger historical trend. This trend is in the process of putting ever-more-powerful technological tools and the knowledge of how to use them into an ever-increasing number of hands. . . . This trend dictates that technology will leverage the ability of individuals and small groups to wage war with equal alacrity. . . . Over time, perhaps in as little as twenty years, and as the leverage provided by technology increases, this threshold will finally reach its culmination- with the ability of one man to declare war on the world and win" (Robb 2007, 8). Finally, there is a preponderance of publications discussing cyber crime. Again, though this is not reflective of the military or warfare, it is still valuable as it provides insights into a similar environment and often common tactics.

Friendly, Environmental, Adversarial

In answering the first secondary research question (see thyself, see the enemy, see the environment)- lessons learned and after action reviews similar to *Network centric warfare case study: U.S. V Corps and 3rd Infantry Division (Mechanized) during Operation Iraqi Freedom Combat operations (March to April 2003)* and *Effects-based operations: applying network centric warfare to peace, crisis, and war* best assess the U.S. Army's current state with respect to reliance on information technology and networks. The network-centric warfare case study consists of three volumes and a multitude of operational examples, to include metrics and data points correlating the

technology to the application. *The New Face of War* by Bruce Berkowitz takes an over-arching approach, much like Robb, yet it correlates its presumptions with historical progression based on insights regarding the people behind prominent defense theory.

To better understand the environment, the Department of Defense *Global Information Grid Architectural Vision* as well as the *Signal Center of Excellence Campaign Plan* offer expectations of the digital infrastructure for the military with specific discussion of Army Divisions and Brigade Combat Teams. However, literature on the Internet as a whole will be reviewed in order to clarify the delicate interaction between financial networks, utility networks, and a vast telecommunications infrastructure. Sources for this perspective are *Black Ice: The Invisible Threat of Cyber-terrorism*; *Indefensible Space: The Architecture of the National Insecurity State*; *Cyber warfare: Terror at a Click*; *Cybercrime, cyberterrorism, cyber warfare: averting an electronic Waterloo*; and *Cyber Threats and Information Security: Meeting the 21st Century Challenge*.

Finally, to gain perspective on the enemy: *Computer Forensics, Incident Response Essentials* and *Hacking Exposed, Network Security Secrets & Solutions* provide insight regarding attack methods and adversarial tactics. *The Development of a Meaningful Hacker Taxonomy* and *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States* discuss first the individuals who will conduct attacks, and secondly, the national approach to utilize those personnel. A number of news media was referenced to gain insight into recent cyber activity throughout the world, specifically regarding China and Russia.

DOTMLPF Analysis

In answering the second research question, the DOTMLPF analysis relied heavily on official publications. The doctrinal references ranged from FM 1-0, *The Army* to FM 3-90.6, *The Brigade Combat Team* while including the operational concepts of Information Operations and Electronic Warfare. The official MTOE for the 1st Brigade, 2d Infantry Division was the centerpiece for personnel and organizational review. This brigade is the only modular formation that continues to focus training on conventional warfighting against nation-state actors, which can be considered the more significant future threat. Training material and leader development references primarily originated from the Fires, Intelligence, and Signal centers for excellence. Throughout the DOTMLPF analysis, it became clear that the Army prefers to focus on this subject matter as the information domain and thus hesitates to embrace "cyber" as a common lexicon. "In the civilian world, the term 'cyber' is used to explain issues representative of the Cyber Age. Over 150 cyber-related terms now exist. On the other hand, in the military world, the focus has remained on using the term 'information' (information operations). . . . Information security, not cyber security, was and remains the key buzzword" (Thomas 2005, 7). As a result, Information Operations became a common thread of discussion in all military references and a number of public works.

Information Operations

In Athena's Camp, Preparing for conflict in the Information Age; *Stray Voltage, War in the Information Age*; *The Next War Zone: confronting the global threat of cyberterrorism*; *Conquest in cyberspace: national security and information warfare*; and *Cyber Silhouettes: shadows over information operations* provide insightful dialogue

regarding the distinction between information operations and cyber warfare. All made some effort to provide historical references (even to antiquity) in order to separate the technical aspects and demystify cyber warfare. The underlying theme for all was that the dynamics between information operations, computer network operations, and electronic warfare is critical to the understanding necessary in order to visualize the future solutions for cyber warfare.

The Battle of Kasserine Pass

In making the historical analogy to the Battle of Kasserine Pass, works from prominent historians (such as Blumenson) were combined with specific insights from the academic community (such as House and Bielakowski) and the narrative prose of Rick Atkinson in the much-celebrated *An Army at Dawn*. Beyond the historical lessons from the Battle of Kasserine Pass, a number of works regarding "innovation" were referenced. *Military Innovation in the Interwar Period*; *The Dynamics of Military Revolution, 1300-2050*; and *Winning the Next War, Innovation and the Modern Military* all offered valuable insight regarding the lessons of innovation and the challenges of institutionalization. The lessons were fully supported with historical events to reinforce their utility to this study.

Key Works

Finally, two key works were: *Dominating Cyberspace* written by U.S. Army War College student Commander Richard Radice in March 2007 and LTG Keith Alexander's June 2007 article in *Joint Forces Quarterly* entitled "Warfighting in Cyberspace." Both summarize the subject in a fashion similar to this thesis, as well as offering realistic

recommendations for military application in the future. As with other references, they do not target the tactical level of war. However, they were extremely insightful and rewarding to examine.

As a final note, though the literature directly addressing cyber warfare at the tactical level was insufficient, I have spent more than ten years as a Signal Officer in the United States Army grappling with these technologies and their practical applications in our profession of arms. That experience was accentuated by duties in a brigade combat team over the last two years. To complement this experience base, I have completed a Bachelor of Science degree in Computer Engineering, a graduate certificate in Telecommunications Management, and a Master of Science degree in Information Assurance. And finally as a measure of my progress with respect to civilian counterparts, I completed the certification requirements for CompTIA's Network+ and Microsoft's Certified Systems Engineer (MCSE). Armed with this body of knowledge, I was confident to make assumptions, synthesize disparate information, and draw conclusions.

This chapter presented the literature analyzed with respect to the questions it addressed. The primary question was broken down by the two secondary questions, and those secondary questions further detailed by tertiary questions. The next chapter relates to the research question by detailing the methodology used to answer it, specifically how the search for answers was conducted. It will explain why the researched items discussed in the previous chapter were chosen. It will take the same approach in its outline of the research method; depicting the process used to analyze each tertiary question in support of their respective secondary questions.

CHAPTER 3

RESEARCH METHODOLOGY

> Problem framing establishes an initial hypothesis about the character of the friendly, adversarial, and wider environmental factors that define the situation.
> — Department of the Army, TRADOC Pamphlet 525-5-500, *Commander's Appreciation and Campaign Design* (2008)

> Doctrine, organizations, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) . . . is a problem-solving construct for assessing current capabilities and managing change.
> — Department of the Army, FM 1, *The Army* (2005)

The primary research question of this study asks this, "Is the Army ready for cyber warfare at the tactical level of operations?" This chapter relates to the research question by detailing the methodology used to answer it, specifically how the search for answers was conducted. The previous chapter presented the literature analyzed with respect to the questions it addressed. The primary question was broken down by the two secondary questions, and those secondary questions further detailed by tertiary questions. This chapter will explain why the researched items discussed in the previous chapter were chosen. It will take the same approach in its outline of the research method; depicting the process used to analyze each tertiary question in support of their respective secondary questions.

The overall structure of this study follows the "what," "so what," "which means," "therefore" argumentative logic. The "what" is obviously the subject matter, the cyber warfare readiness of today's tactical echelon. It will be best represented by the answer to our first secondary research question- is there a cyber threat at the tactical level? Obviously an answer of "yes" elevates the interest in our subject matter. This introduces

the “so what,” and sequence to the second question- are the Division and Brigade Combat Teams ready for this threat? The demonstration of readiness can best be explored by a modified DOTMLPF analysis. With this analysis complete, and both secondary research questions answered, “which means” equates to the answer of the primary research question: Is the Army ready for cyber warfare at the tactical level of operations? Finally the paper can conclude with the “therefore” by fully synthesizing the impact of this subject on the modular force and offering recommendations for the Army.

Friendly, Environmental, Adversarial

The initial onset of research will be directed to answer the question of “what” and identify the nature of the cyber threat. To best understand and present this information, an attempt to gain understanding will start by taking the theoretical approach “know thyself, know thy enemy” popularized by Mao Ze-dong but adapted from the writings of Sun Tzu. The specific teaching was, “Thus it is said: He who knows the other side and knows himself will not be defeated in a hundred battles” (Zi 2003, 77). This translation is echoed in current doctrine as the distinction between an enemy, a party identified as hostile against which the use of force is authorized (FM 3-0 2008, 1-9), and an adversary, a party acknowledged as potentially hostile and the use of force is envisaged (JP 3-0 2008, GL-6). Researching adversaries enables a better analysis within the current operational environment. This analysis will be complemented by an appreciation of the environment with which they both share in an effort to completely frame the problem. To ensure proper context, an explanation of the environment will be sequenced as a segue between the friendly and adversarial discussions.

In order to "know thyself" research in the use of cyberspace by the Army modular force will focus on the Battle Command Systems that directly support a commander's decision cycle and his prosecution of warfare. To best understand the Brigade Combat Team in cyberspace, a study of every digital system that can be applied to the fight must occur. This includes a review of systems or tools that may utilize unclassified networks or those that may not be directly related to Battle Command. The intent is to balance the review on both the technical aspects of a given system as well as the reliance placed on it by the commander's decision cycle.

The primary digital tools operated on the classified (closed) network are referred to as the Army Battle Command Systems (ABCS). The core elements of the ABCS are: Maneuver Control Station (MCS), Advanced Field Artillery Tactical Data System (AFATDS), Air and Missile Defense Workstation (AMDWS), All-Source Analysis System (ASAS), Force XXI Battle Command Brigade and Below (FBCB2), and Combat Service Support Computer System (CSSCS). Systems extending beyond these six primary tools will also be explored briefly. Examples are: Tactical Airspace Integration System (TAIS), Combat Terrain Information Systems (CTIS), Integrated Meteorological System (IMETS), Battle Command Sustainment and Support System (BCS3), Command Post of the Future (CPOF), Global Command and Control System (GCCS), and C2 Data Services. The relevance of these additional systems is not just their inherent connection to the network, but also their relevance to the commander's decision making and overall importance to staff planning and mission execution.

It is also necessary to seek out any secondary tools that are used in direct support to staff functions or periphery tasks. For example, the roles of public affairs, civil affairs,

and staff judge advocate imply a significant interaction with local entities, as well as, an inherent use of unclassified (and potentially unprotected) information streams. It can be expected that similar situations will occur within the sustainment community as resourcing from both commercial or contract providers may occur through their corporate portals on the Internet.

To best understand the tactical posture in cyberspace a review of the environment is necessary. This review will focus on the networks that tie digital systems together. It will discuss the defense networks as well as their interconnectivity with commercial networks- often referred to as the Global Information Grid (GIG). This review will explore the Internet as a whole because it is the environment in which the enemy can operate and discover additional tactics, techniques, and procedures. The relevance of the GIG connectivity with the Internet will be reviewed as part of the discussion regarding secondary tools used in direct support to staff functions or periphery tasks. This aspect of the environment discussion will be focused on weighing the capabilities provided against the inherent risks that result from this connection.

Finally, this study will review the enemy- not at first in the sense of a particular nation-state- but as the persona of the "hacker" and the different skillsets, motivations, and capabilities they comprise. The review will focus on documented "hacker" taxonomy for insight into the various persona that are referred to as "hackers." Additionally, various studies have analyzed significant hacker activities in order to provide the detailed understanding necessary to better defend against future occurrences. These suggestions will be weighed for their perspective applicability during military operations.

Once the "hacker" as a threat is understood, there will be a brief discussion of particular nations that have demonstrated these tactics with the intent of providing situational awareness regarding potential adversaries. Three specific case studies will be reviewed. First, the actions of China against the United States beginning in 2002- collectively referred to as *Titan Rain*. Though specific details are classified, the general nature of the activity provides the ideal opening to this activity as a group effort versus individual action. Second, the hostile cyber actions originating from Russia against the nation of Estonia in 2006. Again, specific disclosure of the participants in this attack are not evident, though the preponderance of information ties it to the Russian hacking community. Even if it was not conducted by the government, it is tied to a nationalist ideal and motivation therefore logically progressing towards a nation-state engagement. Third, and finally, the Russian government actions against the networks and infrastructure of Georgia in coordination with military attacks during the summer of 2008. This analysis should highlight the distinction between actions of a nation-state and those of individuals. More importantly, this final piece of Sun Tzu advice will allow us to answer the "what?" question and progress to the "so what?"

DOTMLPF Analysis

The second research effort will seek to answer the "so what?" question- more specifically, it will ask what has been done to prepare for this new environment and potential threat. Research to answer the question will be organized using a modified DOTMLPF analysis, as it best incorporates the Army's fundamental construct to manage change. An analysis of materiel and an analysis of facility requirements will not be

conducted. This omission is tied to the study's limitation in classification and scope of Division and below organizations.

Research will target published doctrine to determine if the Army has captured both an understanding of what cyber warfare entails and of what our modular force must be prepared to do to properly execute it. This may begin with a review of FM 3-0, *Operations* and Chapter 7 on "Information Superiority." FM 3-0 discusses Information Operations as a major component in achieving this aim, therefore a review of FM 3-13, *Information Operations* will be conducted. FM 3-13 discusses Electronic Warfare as a subordinate element to Information Operations, initiating a review of FM 3-36, *Electronic Warfare*. This is but one example of the potential doctrinal avenues available when exploring mention of cyberspace or cyber warfare. Additionally, strategic documents such as *The National Security Strategy* will be reviewed for any mention of cyberspace or cyber warfare. Though not doctrine by definition, like doctrine, these documents provide guidance to the military. And in some instances this guidance will be reflected in future doctrine, therefore deserving a cursory review.

Research will review organizational structures to critique where current, or potential, cyber warriors will perform duties with respect to the Brigade Combat Team staff or subordinate units. Closely linked with the later personnel analysis, the organizational review focuses on the question of not only who does what, but where within the hierarchy they work. Also, an expression of the duties and responsibilities of their section elaborate on their utilization. An identification of the supervisor in this subset of the organization can be directly tied to the subsequent discussion regarding leader development. The location of cyber warriors within the organization and who

provides them guidance and direction is greatly affected by the preparation leaders are given to satisfy that requirement.

Training will be reviewed to determine how cyber warriors are being developed, and if the effort is sufficient. The learning objectives for both the Advanced Individual Training (AIT) and Basic Noncommissioned Officer's Course for the following specialties will be reviewed: MOS 13F, MOS 25B, MOS 25N, MOS 25U, and MOS 35T. As a reference, the total time typically transpired from AIT completion to BNCOC initiation will be captured. Due to the technical nature of the required skillsets, this timestamp can significantly influence the competence and capability of these soldiers, and thus indirectly impact the unit readiness. Additionally, any programs of instruction (POI) that expound upon these training programs or complement them will be reviewed. To address the mentioned time span between institutional training programs, existing Mission Training Plans (MTP) or Army Training Evaluation Plans (ARTEP) and their application will be explored.

To compliment the training of the cyber warrior, leader development will be critiqued to determine how well they are prepared to make decisions with regard to this emerging capability. This review will focus on the officers of MOS 13A (Field Artillery), officers of MOS 35G (Military Intelligence), and officers of MOS 25A (Signal Corps). The learning objectives documented as part of the training curriculum for the Basic Officer's Leader Course and the Captain's Career Course will be the basis for this portion of analysis. It will also conduct the same review for the following Advanced Noncommissioned Officer Courses: MOS 13F, MOS 25B, MOS 25N, MOS 25U, and MOS 35T.

Finally, research regarding personnel will review existing MTOEs to identify the number of cyber warriors currently serving in the modular force and the aforementioned organizations. This will include a review of any force design update (FDU) or proposed changes to the MTOE. This discussion may be offered within the organizational and leader development analysis if it better compliments those areas. As previously stated, the Brigade Combat Team and Division headquarters best represent the tactical nature of the U.S. Army and therefore will be the only MTOEs scrutinized for personnel authorization details. The completed DOTMLPF analysis yields the "so what" to give us an understanding of how well the Army has postured our fighting force for the "what" which means we can then answer the primary research question.

This chapter explained why the researched items were chosen by outlining the research method; depicting the process used to analyze each tertiary question in support of their respective secondary questions. The next chapter provides the meta-analysis of the research material detailed in the second chapter's literature review. In short, it provides the answers that were found. It will present analysis using the same construct as before: the primary question was broken down by the two secondary questions, and those secondary questions further detailed by tertiary questions.

CHAPTER 4

ANALYSIS

> Peace really does not exist in the Information Age.
>
> — Lt Gen. Kenneth Minihan
> Director, National Security Agency
> June 1998

> UBL [Usama bin Laden] took technology and used it to his advantage faster than we [did].
>
> — Larry Castro
> Director of Homeland Security, National Security Agency
> August 2002

The primary research question of this study asked, "Is the Army ready for cyber warfare at the tactical level of operations?" This chapter relates to the research question by providing the meta-analysis of the research material detailed in the second chapter's literature review. In short, it provides the answers that were found. The previous chapter explained why the researched items were chosen by outlining the research method; depicting the process used to analyze each tertiary question in support of their respective secondary questions. This chapter presents the analysis using the same construct as before: the primary question was broken down by the two secondary questions, and those secondary questions further detailed by tertiary questions.

Friendly, Environmental, Adversarial

The initial secondary research question asked, "Is there a cyber threat at the tactical level?" Friendly connotations for cyber warfare are best determined by an introspection of the Army's view of information; both a respect for and use of information. Rather than be limited by the definition of an enemy, adversaries were

researched as they represent the documented opposition that falls outside the realm of defined enemy forces. The analysis was complemented by an appreciation of the environment with which they both share in an effort to completely frame the problem and quantify the supposed threat.

Friendly

The Army modular force will focus on the Battle Command Systems that directly support a commander's decision cycle and his prosecution of warfare. To best understand the Brigade Combat Team in cyberspace, every digital system that can be applied to the fight must be seen for its role in supporting the commander's decision cycle. This includes a review of systems or tools that may utilize unclassified networks or those that may not be directly related to Battle Command if they also contribute to the commander's ability to "understand." During Operation Iraqi Freedom, "commanders stated that they made better decisions more quickly because of the timeliness and accuracy of information they had readily available to them" (Cammons 2008, 31). The reliance placed on a digital system by the commander's decision cycle will prioritize the technical aspects that govern its connectivity.

The primary digital tools operated on the classified network are referred to as the Army Battle Command Systems (ABCS). The core elements of the ABCS are: Maneuver Control System (MCS), Advanced Field Artillery Tactical Data System (AFATDS), Air and Missile Defense Workstation (AMDWS), All Source Analysis System (ASAS), Force XXI Battle Command Brigade and Below (FBCB2), and Combat Service Support Control System (CSSCS). When incorporated into Battle Command during Operation Iraqi Freedom, the new information environment encouraged maneuver aggressiveness or

boldness synchronized with precision fires. Leading the charge to Baghdad as Commander of 3rd Infantry Division, MG Blount described that "increased situational awareness and the lethality of our systems gave me the confidence to take additional risk" (Cammons 2008, 41). These systems translated higher levels of shared battlespace awareness into increased combat power and directly affected command decisions.

The Command Post of the Future (CPOF) has emerged as the system of systems used to better interface the ABCS. The CPOF has created a niche as a commander's tool, providing the ability to access the work of the various warfighting functions while establishing a shared workspace with senior or subordinate commanders. Additionally, the C2 Data Services system is currently being tested for acceptance decision in summer of 2009. The C2 Data Services system is designed "to provide near real-time tactical edge-to-Combatant Command (COCOM) collecting, managing, sharing and exploiting of human-derived information . . . standardizes the format of the information from the team/squad to the Global Information Grid" (Bob Hartel, U.S. Army CAC Blog, entry posted March 16, 2009). Linking the senior commander in a theater to the lowest tactical echelon is quite audacious, yet regardless of the logic in its occurrence the demonstration of capability will provide a watershed moment. The relevance of these systems is not their physical connection to the network, but their criticality to the commander's decision making process and overall importance to staff planning and mission execution.

Systems extending beyond the six primary tools of ABCS will be explored briefly. Examples are: Tactical Airspace Integration System (TAIS), Combat Terrain Information Systems (CTIS), Integrated Meteorological System (IMETS), Battle Command Sustainment and Support System (BCS3). As the planning tool for airspace,

TAIS provides a safety mechanism for a high-risk environment. Though it may not be part of the Common Operational Picture (COP), its role in de-conflicting battlespace prior to execution is critical. CTIS and IMETS assist the staff in providing an accurate representation of the environment for a commander and are instrumental in planning. BCS3 is one of the only logistics platforms that utilizes secure networks making it a focal point for accurately representing the real-time sustainability of the force. The other systems, those that are getting the work done, typically operate on the nonsecure networks to interface with the immense support community.

Use of nonsecure networks goes beyond the service and support elements of the BCT. The newly formed Information Operations section, previously referred to as non-lethal effects, must strike a balance between the combat situation and perception of a local populace. For example, Public Affairs personnel require a connection to the Internet in order to maintain currency in events reported by local, regional, and international media. The Internet will also provide the requisite transmission medium for stories or news reports to be submitted to various media outlets. Civil Affairs personnel will be expected to establish communications with civic entities that lack tactical radios or classified information systems. They will be constrained to correspondence via the Internet and commercial electronic mail applications. The Staff Judge Advocate utilizes the Internet to research specifications of the Law of Armed Conflict (LOAC) and legal precedence for the Uniform Code of Military Justice (UCMJ). Each of these staff proponents offer critical advice to the commander and in some fashion shapes his decisions. However, this subset of secondary systems has the potential to become the

Achilles heel of a tactical units' information infrastructure if there is a present cyber threat.

The National Military Strategy states that "a campaign to win decisively will include actions to destroy an adversary's military capabilities through the integrated application of air, ground, maritime, space, and information capabilities" (Myers 2004, 14). It will require "a networked force capable of decision superiority . . . information from the national to tactical levels . . . to decide and act faster than opponents" (Myers 2004, 16). The information capabilities were discussed in the overview of friendly considerations, yet the "networked force" compels a better description of the global information grid and the military interfaces to the Internet.

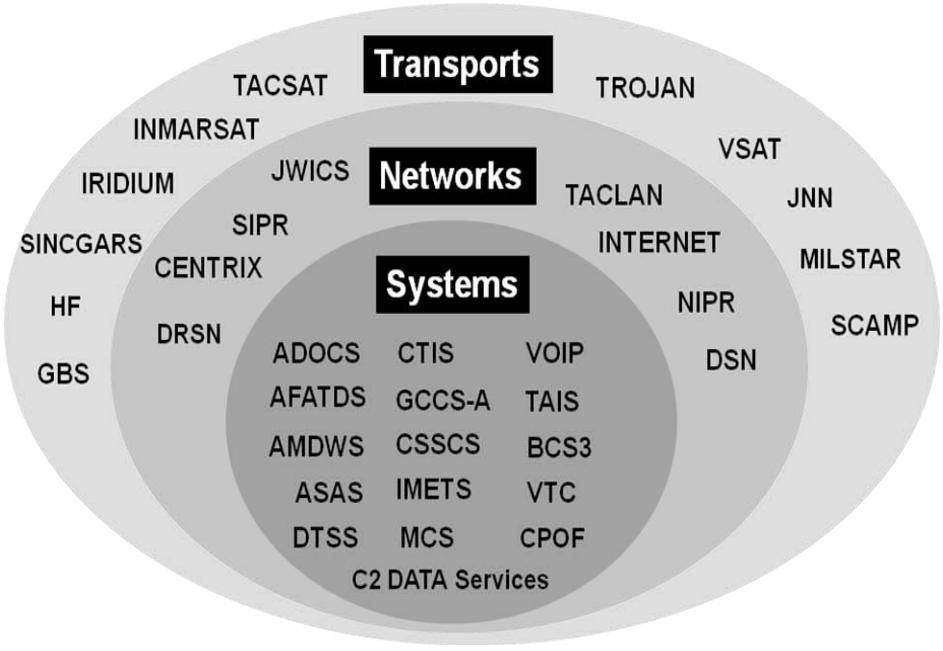

Figure 1. Friendly Information Infrastructure
Source: G6, 2ID, "C4 Capabilities Brief," Camp Red Cloud, ROK, January 2006.

Environmental

One of the functions and responsibilities of the Department of Defense is the "integration of the Armed Forces into an effective and efficient team operating within the air, land, maritime, and space domains and the information environment" (JP 1-0 2007, III-2). The Deputy Defense Secretary defined cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (England 2008, 1). In doing so, he combined the physical system of interconnected computer networks with the virtual system of data found in web pages to quantify an information environment. More importantly, he defines cyberspace as a global domain which equates it to land, air, sea, and space.

The environment of military networks has two primary entities; the NIPRNET and SIPRNET. The Nonsecure Internet Protocol Router Network (NIPRNET) is a system of computer networks used to exchange unclassified but sensitive information between "internal" users as well as providing those users access to the Internet. Conversely, the SECRET Internet Protocol Router Network (SIPRNET) is a system of computer networks used by the Department of Defense to transmit classified information (up to and including classified SECRET). These two networks are physically separate as a means of securing the distinct levels of classification they support. The SIPRNET is the de facto network used in combat operations; however, both are utilized in the tactical environment. The connectivity of the NIPRNET to the Internet is the aforementioned Global Information Grid (GIG).

In 2002, Army General Order #5 mandated that all Army networks fall under the technical oversight of the Network Enterprise Command (NETCOM)- a direct reporting unit to the Army CIO / G6. Specifically, NETCOM "is the single authority assigned to operate, manage, and defend the Army's 'Infostructure' at the enterprise level . . . operates, sustains, and defends the Army's portion of the Global Information Grid . . . will deliver 'seamless' enterprise level Command, Control, Communications, Computers, and Information Technology common user services and signal warfighting forces" (White 2002, 2). Additionally, DoD Directive 8100.1 made compliance with the GIG architecture mandatory for all voice, data, and video products for combat operations. Both policy efforts are results of the realization that strict controls must be in place to gain any posture of security in an entity as complex as the GIG.

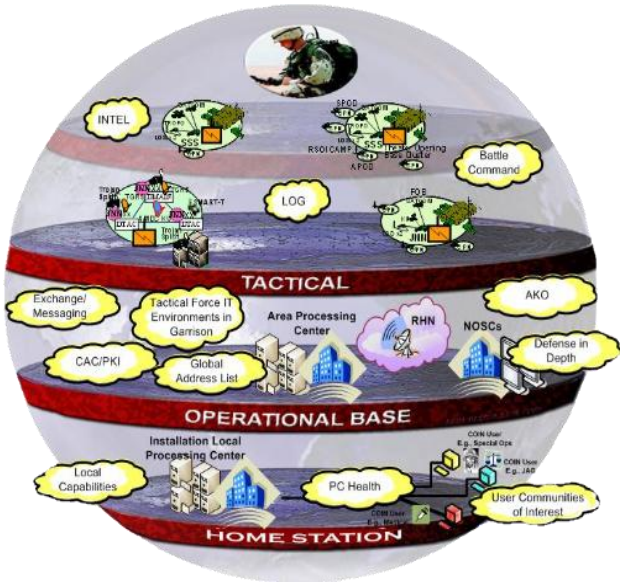

Figure 2. Global Information Grid (GIG)
Source: NETCOM, "Command Brief," Ft. Huahchuca, AZ, September 2007.

The GIG connectivity facilitates secondary tools used in direct support to staff functions or periphery tasks by enabling access to the Internet. This aspect of the environment forces a planner to weigh the capabilities provided against the inherent risks that result from this connection. "Security within the twenty-first century will require a new balance. . . . The balance is increasingly between preserving the benefits of global interconnectivity and insulating against the myriad of threats that can strike at us through those same connections" (Robb 2007, 152). For the military, the Internet connection to the GIG can be visualized as the enemy high-speed avenue of approach in a cyber attack.

It is important for the military to remain cognizant of the commercial characteristics of networking. "A major hurdle that nations face in defending their critical infrastructures is working with entities that control telecommunications networks, electrical grids, and transportation systems. This is a significant issue in the United States, given that the private sector owns more than 85% of the critical infrastructure" (Gaudin 2007, 49). But beyond defending the network, corporations seeking profitability must remain at the cusp of technological performance. Therefore, the corporate aspects of the Internet are often forced to balance profit and security. The coupling of an extensive commercial network and the military's effort to incorporate current and emerging technologies into its network means the vulnerabilities identified in the Internet are most likely vulnerabilities in our GIG. It is a fact that the growth of a computer-literate population (implying a greater pool of potential "hackers"), the inherent vulnerabilities of common protocols in computer software and networks, the easy availability of "hacker" "toolkits" (available on many websites), and the fact that the basic tools of the "hacker"

(computer and network access) are the same essential technologies used by the general population make this a dangerous environment (Moteff 2001, 49).

Adversarial

A study into cyber warfare finds its logical precursor in cyber crime. Similar tactics, techniques, and procedures employed between different opposing forces. If we do not encounter cyber warfare in its true form (such as against a nation-state) we will be confronted by cyber terrorism (cyber warfare against a nonstate actor). Either form benefits from reviewing the history of cyber crime. Cyber crime is typically characterized by the term of "hacker" as a "super-genius sitting alone at a keyboard in the early dawn hours, hammering away like a grand maestro to exploit an undiscovered technical flaw in the digital armor of the world's largest corporations" (McClure et al. 1999, 4). Unfortunately this single stereotype is not far from the current legal opinion. According to Professor Marcus Rogers, "the use of one generic category is analogous to attempting to understand criminal activity by lumping the entire spectrum of traditional criminals (i.e. shoplifters to homicidal psychopaths) into one generic group . . . this is what we are currently doing with the criminal domain of computer crimes" (Rogers 2005, 3). Rogers suggests the "dreaded enemy of the Internet and the new globally connected society" be better understood than the simple "hacker" label and offers a taxonomy to do so.

Rogers offers eight categories to best quantify technical abilities and motivations, in order from lowest to highest: *Novice*, *Cyber Punks*, *Internals*, *Petty Thieves*, *Virus Writers*, *Old Guard Hackers*, *Professional Criminals*, and *Information Warriors* (Rogers 2005, 2). Though this threat spectrum seems broad, it accurately depicts the adversaries mentioned in most literature as populating the cyber domain. *Internals*, for example,

represent a significant risk because they are present in all organizations and have legitimate access to networks. Roughly 75 percent of computer crime loss is attributed to approved users, with 19 percent caused by either dishonest or disgruntled employees and 55 percent to human error (Bragg et al. 2004, 35).

Novices are also referred to as "script-kiddies" because they typically have limited skills and are reliant on "pre-written pieces of software, referred to as tool kits, to conduct their attacks. The 'tool kits' are readily available on the Internet" (Rogers 2005, 3). A similar term, "root kit," describes sets of modified system binaries providing hackers backdoors for future access (Kruse and Heiser 2002, 127). Anyone can use a "tool kit" to exploit a system, where as a "root kit" is placed after a system is penetrated to ease or mask future unauthorized access. A *Novice* usually does not utilize "root kits" because they are often just exploring the Internet to satisfy inner deviance and curiousity. Just a step above, *Cyber Punks* represent a greater degree of skill, if not in the writing of destructive code than in the basic understanding of the systems they are targeting. This advanced level of understanding allows them to often use "root kits" and maintain access to desired systems. *Cyber Punks* are almost synonymous with *Petty Thieves* regarding skill sets, just differing in their motivations. *Cyber Punks* exude computer deviance and continually seek out attention at the expense of others, while *Petty Thieves* remain anonymous and preserve their occupation.

Old Guard Hackers, *Professional Criminals*, and *Information Warriors* are a significant threat in the cyber domain. *Old Guard Hackers* center themselves on ideology and challenge. They create the "toolkits" used by others, and though they rarely use them they readily make them available and encourage their use. Due to their ideological

extremes, this community may be potential cyber terrorists answering the call for a digital jihad. Similar considerations are given to *Professional Criminals* and *Information Warriors* who are often "for hire" and therefore can be employed to target the United States Army. *Information Warriors* are considered to be ex-intelligence operatives (Rogers 2005, 4) and therefore can be considered an equivalent to a state actor in conventional cyber warfare.

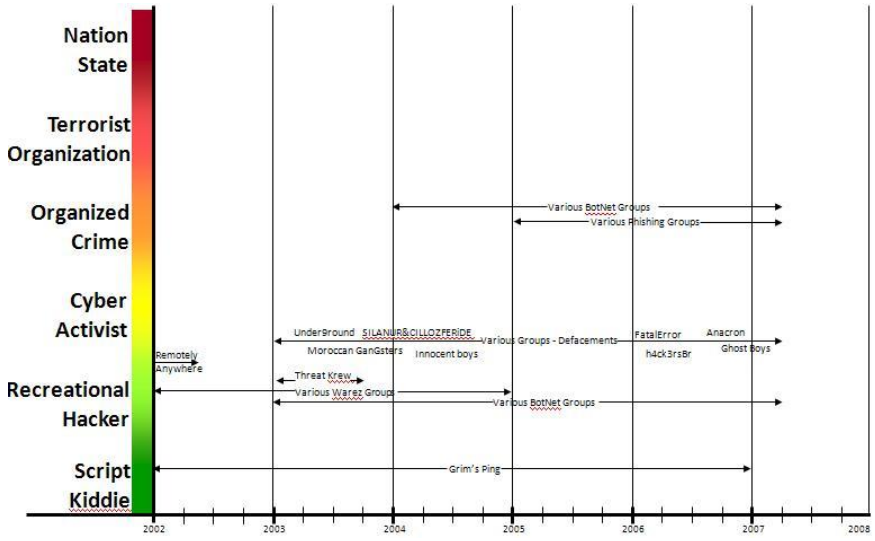

Figure 3. Threat Actors
Source: RCERT-CONUS, "Threat Brief," Ft. Belvoir, VA, April 2009.

Officials indicate that more than 20 countries have various kinds of Information Operations (IO) directed against the United States. A declassified Navy threat assessment identifies Russia, China, India, and Cuba as countries who have acknowledged policies of preparing for cyber warfare and who are rapidly developing their capabilities (Hildreth 2001, 2). In China specifically, "the People's Liberation Army (PLA) has formulated an

official cyber warfare doctrine, implemented appropriate training for its officers, and conducted cyber warfare simulations and military exercises" (Billo and Chang 2004, 7). China's military is not the only concern. "One of the unique aspects of the Chinese hacker organization is their nationalism, which is in stark contrast to the loner or anarchist culture many associate with the stereotypical Western hacker. They are especially active during periods of political conflict with other nations" (Henderson 2007, ix). The current competitiveness of China as a world power enhances projections of them as a cyber threat; either in the form of a state or non-state actor.

In 1998, two Chinese PLA Colonels authored a military manual titled *Unrestricted Warfare*. The manual depicted a plan to destroy America with deliberate, psychological, criminal, financial, and commercial acts undertaken by a state or nonstate actor, with specific mention of terrorists and hackers. The manual gained prominence after September 11 due to its references to Osama bin Laden and the bombing of the World Trade Center. In 1999, the Pentagon "detected some 22,000 attempts to hack into their systems. . . . In 2000, there was about a 10% increase... successful ones were traced back to military organizations in China" (Dunnigan 2003, 88). In 2003, a series of Chinese cyber attacks against the U.S. was labeled *Titan Rain* (Norton-Taylor 2007, 3). Though precise origins of the attack, as well as the exact methods of the attack, have not been disclosed, *Titan Rain* provided the international community with the first possibility of a cyber attack from a nation-state.

Similarly, two instances of cyber warfare captured the military community's attention. In 2007, the government of Estonia was crippled by assumed Russian cyber attacks (Marsan 2007, 22). More importantly, this attack gave the first glimpse of cyber

being used to impart a military effect as it resembled the cyber version of a military air campaign. The attacks disrupted a dozen government Web sites and networks run by various service providers, financial institutions and media outlets for several weeks. Pro-Russian activists were behind the cyber attacks, supposedly motivated by the Estonian government's decision to move a Soviet World War II memorial (Marsan 2007, 1). The targeting of a government immediately suggests cyber warfare; however, the origination by nonstate actors motivated by a sense of nationalism reiterates the danger of skilled individuals with motivations to prosecute their frustrations in cyberspace. It is hard to completely dismiss the possibility of government participation as Russia's armed forces are known to have extensively coordinated with IT sector experts and the academic community while developing their cyber warfare doctrine (Billo and Chang 2004, 9).

Shortly thereafter in 2008, similar actions took place in the country of Georgia. Of specific interest, the actions against Georgia occurred in concert with military operations against the country. If the world questioned the previous events and their purpose, Georgia erased all doubt and demonstrated the signature of cyber warfare. Russian military forces moved into Georgia while the government suffered the desperation of a crumbling infrastructure, both virtual and physical. "It is extremely difficult to sort out which hacks are being done with Russian government involvement, which are being done with government wink-and-a-nod, and which have nothing to do with the government whatsoever" (Shachtman 2008, 1). However, there is a Russian concept of "information weaponry" which "receives paramount attention in official cyber warfare doctrine" (Billo and Chang 2004, 9). If the government was not involved, the possibility of nationalizing an indigenous "hacker" force to support the military's current operations is quite

intriguing. Either way, the lesson lies in the effect found in synchronized maneuver in both the land and cyber domains.

The analysis of the friend, foe, and their shared environment answered the question of "what" by identifying the nature of a likely cyber threat at the tactical level. The Army's view of digital systems to support information as the critical factor of a commander's decision cycle, weighed against the varied adversaries that can confront the modular force in cyberspace best represents what will eventually become cyber warfare at the tactical level. This realization compels the "so what" question regarding what has been done to prepare for this new environment and potential threat. Answering this second question required a modified DOTMLPF analysis and is the final step in responding to the primary research question, "Is the Army ready for cyber warfare at the tactical level of operations?"

DOTMLPF Analysis

Analysis of the previous question demonstrated a legitimate cyber threat and set the expectation for how prepared the Division and Brigade Combat Team needs to be to operate in cyberspace. The second question asked, "has the U.S. Army prepared Divisions and Brigade Combat Teams for the execution of cyber warfare?" This question is explored through a modified DOTMLPF analysis, as it best incorporates the Army's fundamental construct to manage change. As outlined in the previous chapter, an analysis of materiel and an analysis of facility requirements was not conducted. This exclusion is tied to the study's limitation in classification and scope of Division and below organizations. Even with these omissions, the effort can adequately answer the "so

what?" question- more specifically, what has been done to prepare for this new environment and anticipated threat.

Doctrine

Doctrine is an authoritative statement regarding how elements of the Army contribute to operations; not hard and fast rules but a guide to action that provides a common reference across the force (FM 1-0 2005, 1-78). FM 1-0, the first of the Army's capstone manuals, introduces two broad concepts that acknowledge the cyber threat identified in the previous section. FM 1-0 discusses new adversaries, methods, and capabilities in the construct of traditional, irregular, catastrophic, and disruptive (FM 1-0 2005, 2-9). The cyber threat can be characterized by any of these descriptions within a tactical context, though catastrophic seems more appropriate at the strategic level. The capability goal of "developing networked information systems" expresses that the Army must provide networked information systems down to the lowest level and reinforces command expectations of information superiority (FM 1-0 2005, 4-31).

Representing the first revision since the events of September 11, 2001, the February 2008 release of FM 3-0, *Operations*, acknowledges a changed world with new threats to our national security and recognizes the challenges of full spectrum operations. FM 3-0 expands upon the FM 1-0 description of the adversarial challenges by offering insight into that specific threat's impacts on operations. And though FM 3-0 continues to echo the necessity of additional networked information systems to facilitate the 'common operational picture' (COP), it dedicates an entire chapter to the concept of information superiority in order to fully communicate and visualize the role of information in the operational environment.

Chapter 7 of FM 3-0, "Information Superiority," provides the most detailed discussion of cyber elements as it tackles the criticality of dominance in the information domain. Information superiority is defined as the ability to collect, process, and disseminate information while exploiting or denying an adversary's ability to do the same (JP 3-13 2007). FM 3-0 further details four contributors to information superiority: Army information tasks; intelligence, surveillance, and reconnaissance (ISR); knowledge management; and information management. The explanation of all four reinforces the analysis of friendly, adversarial, and environmental factors previously discussed.

Army information tasks are simply intended to protect friendly information and attack opponents or threats. They are information engagement, command and control warfare, information protection, operations security, and military deception. Command and control warfare is the integrated use of physical attack, electronic warfare, and computer network operations to deny, degrade, or destroy the enemy's command and control capabilities (FM 3-0 2008, 7-24). Command and control warfare further encapsulates responsibilities for electronic warfare, electronic attack, electronic warfare support, and computer network operations. A second task, information protection is the measures taken to defend friendly information and information systems from enemy influence (FM 3-0 2008, 7-31). Information protection includes information assurance, computer network defense, and electronic protection.

The elaboration on intelligence, surveillance, and reconnaissance responsibilities does not explicitly discuss a cyber component. Additionally, knowledge management implies the extensive use of information systems and networks while focusing more on the processes than the infrastructure. Information management begins the dialogue

regarding the infrastructure and also emphasizes the need to protect and defend the information and information systems. These two management areas tie closely to the previous discussion regarding the Army's friendly and environmental cyber considerations. In doing so they reiterate both the reliance commanders will be forced to place on cyber capabilities and the vulnerabilities that are inherent in them. This is the overarching message one would expect to gain from a capstone manual, basically setting the stage for other publications.

FM 3-13 is the Army's Information Operations doctrine. Acknowledging information as an element of combat power and information security as the execution of that element, it expounds further on what Chapter 7 of FM 3-0, "Information Superiority," introduced. The initial draft revision of FM 3-13 (dated 27 Feb 09) contains a chapter entitled "Gaining and Exploiting the Operational Advantage in the Effective Use of Information Technology Networks." Within this draft chapter cyberspace and network warfare are defined; the first instance in Army doctrine. Additionally, it frames the context for full spectrum operations by stating "information is the currency of understanding, decision-making, and action while cyberspace is a domain in the operational environment in and through which cognitive and physical effects can be created" (FMI 3-13 2009, 4-9). However, since this is a draft publication it does not constitute approved doctrine and analysis must revert to the current published version.

Published in 2000, FM 3-13 explains that Information Operations are executed using twelve elements: operations security (OPSEC), psychological operations (PSYOP), counterpropaganda, military deception, counterdeception, electronic warfare, computer network attack (CNA), physical destruction, information assurance, physical security,

counterintelligence, and special IO (FM 3-13 2000, 1-35). It recognizes both offensive and defensive incorporation of these elements. In its first chapter, FM 3-13 begins to introduce potential adversaries and threats, providing the first doctrinal use of the terms "insiders" and "hackers" as well as "logic bombs" and "viruses." It even mentions foreign intelligence services as a potential threat. Though the terms are not explored in depth, the mention correlates with the adversarial descriptions provided earlier. The manual also provides a clear distinction between electronic protection, a subordinate element of electronic warfare, and information assurance (network protection). Similarly, electronic warfare's subordinate arm of electronic attack is separated from the discussion of computer network attack. Addressing cyber activities discretely from electronic warfare reveals an interesting trend that continues in FM 3-36.

FM 3-36 is the Army's doctrine for Electronic Warfare (EW). It reiterates the three basic functions of electronic protect, electronic support, and electronic attack in its support to full spectrum operations. The manual revisits the concept of information superiority and provides further detail regarding the information operations elements under its oversight. What it avoids is discussion of computer network operations. There is no mention of network warfare or a single instance of the term cyber. The reader is left to imply cyber connotations to the subject matter of electronic warfare, or view it as a separate and distinct discipline. This is in direct contradiction to the manual's foreword which states "FM 3-36 is moving the Army's EW strategy forward into cyberspace" (FM 3-36 2009).

FM 3-90.6, *The Brigade Combat Team*, was published in 2006 and considered the reflection of Army Transformation and the guidance for modularity's centerpiece. In this

subject area it emphasizes the role of newly fielded communications technologies and the synergy between echelons facilitated by networks. It echoes the previous discussion regarding friendly considerations. However, the term ‘cyber’ is not used nor is the environment mentioned. Similarly, little note of electronic warfare is discussed in the S2 Intelligence verbiage or note of information protect functions in the S6 Communications section. Under the fire support descriptions, a nominal ‘electronic attack’ officer is provided responsibilities. The manual highlights the Information Operations Section and the provision of offensive and defensive IO advice and coordination, but there is little depth for reference. In short, guidance for BCT operations is doctrinally limited to IO considerations and will only prove relevant if complemented by a reading of FM 3-13.

Doctrine focuses on how to think- not what to think (FM 3-0 2008, D-1). It establishes how the Army views the nature of operations, the fundamentals by which Army forces conduct operations, and the methods by which commanders exercise command and control. Outside of the expectations it sets in leaders and units regarding the operational environment, it forms the basis for training and leader development of the force. Doctrine furnishes the intellectual tools with which to diagnose unexpected requirements. It also provides a menu of practical options based on experience from which self-aware and adaptive Army leaders can create their own solutions quickly and effectively (FM 1-0 2005, 1-80). Based on this analysis, current doctrine is not entirely relevant to the previously demonstrated threat environment. Though information operations admittedly demonstrates more discourse than cyber operations, there is progress to be made if BCT Commanders are expected to leverage cyber capabilities in their prosecution of warfare.

Organization

The Brigade Combat Team is the organizational construct most appropriate for analysis of readiness at the tactical level as it is the centerpiece of the modular force. Based on the aforementioned discussion of doctrine, connotations of cyber warfare will be found in the Fires and Effects Cell of the S3 Section (Operations), the S2 Section (Intelligence), and the S6 Section (Communications). Judgment is often passed on an organizational construct by a simple critique of the Military Occupational Specialties (MOS) authorized. This study went a step further by exploring the hierarchical relationships within the organization to determine if the expectations on leaders were inordinate because of the varying competencies required.

The Brigade Combat Team headquarters is designed with an S7 Information Operations Section. Previously referred to as "non-lethal effects," it contains officers and NCOs of the various IO subdisciplines. Specifically, an FA30 (Information Operations) Major, an FA27 (Operational Law) Major, and an FA38 (Civil Affairs) Major. In some instances, the FA49 (Public Affairs) Major will be co-located, or in the immediate vicinity, to ensure congruence of "message." Within this section there is an authorization for a 35G (SIGINT) Electronic Warfare Officer at the rank of Captain. This is the sole individual from the Intelligence proponent within the Information Operations Section. There are no authorizations from the Signal proponent (25). There is a 131A (Targeting) at the rank of Chief Warrant Officer 3 and four 13F (Fire Support Specialists). The presence of the Fires proponent is interesting considering "electronic attack is not performed at the brigade level" (FM 3-13 2000, F-20). This is not an estimate of its possible occurrence, but a reference from the current published doctrinal guidance.

The S2 Intelligence Section is entirely composed of specialties from the Intelligence proponent. However, none of those personnel are identified as holding SIGINT / Electronic Warfare skills. The Military Intelligence Company (MICO) often augments the Brigade S2 Section, though it technically falls subordinate to the Brigade Special Troops Battalion (BSTB). The company has a 353T (IEW Technician) Warrant Officer assigned and a number of 35N (SIGINT Analyst). The majority of the 35N positions are assigned against the PROPHET systems organic to the company, and therefore would not likely be found at the Brigade-level contributing to a potential cyber war. However, it is doctrinally sound for the MICO to establish a Fusion Cell co-located with the Brigade S2 at the Brigade Tactical Operations Center (TOC). This makes all organic assets immediately available to the senior Intelligence Officer in the brigade and allows the organization to tailor support in the best interests of the Brigade Commander.

The S6 Communications Section is also entirely composed of specialties from the Signal proponent. However, more than Intelligence, the Signal occupational specialties correlate directly to networks and the cyber domain. The FA25 (Signal) Major is complimented by an FA53 (Information Systems) Captain, and a 254A (Signal Systems Support Technician) Warrant Officer. The remainder of the S6 Section is composed of 25U (Signal Support Systems Specialist) and 25B (Information Technology Specialist) personnel. The Network Support Company (NSC) organic to the BSTB contains a Network Operations (NETOPS) cell led by a 250N (Network Management Technician). It is composed of 25B, 25S (Satellite Operations), 25F (Network Switching Specialist), and 25E (Electromagnetic Spectrum Manager). Similar to the MICO, the NETOPS cell augments the S6 area within the Brigade TOC. Again, these additional personnel become

immediately available to the senior Signal Officer in the brigade and allows the organization to tailor support in the best interests of the Brigade Commander.

The S3 Fires Coordination cell is entirely composed of specialties from the Fires proponent, primarily 13F personnel. FM 3-36 prescribed the components of Electronic Warfare to be evident in the S3 Fires, S2, and S6 sections. S3 Fires would oversee and implement electronic attack, S6 Communications would oversee and implement electronic protect, and S2 Intelligence would oversee and implement electronic support (and exploitation). This analysis finds the current organizational structure and personnel authorizations to be a feasible approach for the Brigade Commander, with the additional flexibility of directing the S7 Information Operations to address electronic attack. However, this organizational structure is reliant on whether or not these Military Occupational Specialties have conducted the institutional training to perform the necessary tasks.

Training

Training and Doctrine Command (TRADOC) has the responsibility to establish the overall training continuum for all military occupational specialties. To build upon the aforementioned organizational review, a study of the critical competencies for the targeted military occupational specialties demonstrates the skillsets with regard to cyber warfare that those personnel bring to the organization. Accordingly, the absence of required competencies is also noted for consideration.

Aside from the anticipated "execute fire support" task, the 13F is required to perform only one additional function that could contribute to cyber warfare: coordinate for non-lethal assets (13F STP 2004, 3-462). It is a task to be instructed at the Advanced

Noncommissioned Officer Course (ANCOC). There are no additional tasks in the MOS training plan which directly relate to information operations or electronic warfare. However, recent lessons learned indicated that "some IO tasks in Iraq and elsewhere, for example, were assigned to the artillery personnel because they understood targeting, no IO theory and practice" (Thomas 2005, 8). Indirectly, the tasks required in support of executing the targeting process could be utilized. Electronic attack and computer network attack procedures need to mirror the accepted targeting cycle for the brigade.

The 35G (SIGINT) training continuum contains three critical tasks that relate to information operations or electronic warfare: conduct electronic warfare, define computer network operations, and define the current and emerging signals environment (Smith 2008, 1). Conducting electronic warfare entails a review of the target area technical data to develop methods of collection and exploitation, an examination of the organization's organic and supporting SIGINT/EW architecture to determine systems available for utilization, and the development of the Electronic Warfare (EW) Annex (Smith 2008, 13). Defining computer network operations requires an understanding of the elements of computer network attack, computer network exploitation, and computer network defense with the identification of existing network components, data paths, end points, and protocols (Smith 2008, 15). Finally, defining the current and emerging environment requires the soldier to identify communications in the Area of Interest (AI), the impact of emerging technology for exploration or destruction, whether the technology is involved in the target's deception or denial operation, and feasibility of acquiring and incorporating the technology into friendly operations. These training plans are a marked improvement when compared to the published doctrine.

The 25B training continuum is a consistent stream of network principled tasks that center on the cyber domain. The underlying purpose is provision of services and information management. 25B personnel are the "help desk" of the brigade headquarters and therefore receive a large proportion of training focused on the software of information systems and associated user interfaces. The "defend" tasks are based in configurations and policy. The training continuum is similar for both the 25F and 250N specialties; however, these personnel focus more on the network components and technical specifications. There is a "defend" or "protect" task associated with each equipment item. Both enlisted MOS feed into the warrant officer specialty of 251A. The 251A Warrant Officer Basic and Advanced Courses both review the 25B and 25F tasks with a culminating capstone exercise requiring graduates to install a "secure" Brigade Command Post (Kulifay 2002, 31). A capstone exercise of this fashion clearly demonstrates the expectation leaders have of these personnel once they arrive to their units.

There is room for improvement regarding the training framework to develop cyber warriors. However, before this training construct can be developed a doctrinal understanding of executing cyber warfare must be clearly established. As a premature concept, any attempt to force untrained personnel into the cyber domain could have negative impacts on critical information systems and processes. Yet training at this early stage in institutionalization will need to be comprehensive as personnel will likely be mismanaged and forced to work above their rank and grade. Just as the institutional training requires time to grasp cyber warfare, the personnel management system will face the same challenges as it provides soldiers, as well as leaders, to the modular force.

Leader Development

As discussed previously, the organizational study explored the hierarchical relationships within the organization to determine if the expectations on leaders were inordinate because of the varying competencies required. The competencies of officers and senior NCOs was scrutinized to determine the flexibility in executing the various tasks projected for the cyber environment.

Signal officers receive training in the installation, operation, maintenance, and defense of networks during the Signal Officer Basic Course. This training is advanced at the Signal Captain's Career Course with a Signal Management Exercise in which students execute an Information Assurance Plan (Brown, SCCC POI 2006b, 4-41). Finally, the Battalion S6 Course has an entire module on C2 Protect Tools which combines instruction with a hands-on laboratory learning environment (Brown, BN S6 POI 2006a, 4-12). The officer training continuum adequately addresses the dynamics of the cyber domain with respect to the doctrinal responsibilities previously discussed.

Though there are no specific references to the cyber domain in 13 and 35 series officer courses, the Fires proponent familiarizes officers with non-lethal effects and basic Information Operations functions. The Intelligence proponent addresses electronic warfare in depth for selected officers. To address the gap evident within these two communities, the Operational Electronic Warfare Course (AOEWC) was established. In response to an emerging requirement for Brigade-level and higher Electronic Warfare Officers (EWOs) in support of current operations in OIF and OEF, graduates are awarded the 1J Additional Skill Identifier (ASI). This corresponds to an operational requirement for brigade and higher units deploying into theater to have 1J trained personnel on staff.

AOEWC graduates have a working knowledge of electronic warfare fundamentals, Joint and Army Electronic Warfare capabilities, and integration of EW into the Military Decision Making Process (MDMP), and the targeting process (Funk 2008, 15).

Additionally, Fort Sill launched the "pilot" course of the Functional Area 29 Officer Qualification Course in June 2008. Functional Area 29 is a new Army Functional Area focused on Command and Control Warfare (C2W) and Electronic Warfare (EW) (Funk 2008, 15). It is not evident if the new functional area will supplant the existing 35G Electronic Warfare Officer authorized within the brigade headquarters or if this development signifies growth for the position below the brigade level. Regardless, creation of a new functional area and corresponding enlisted military occupational specialty indicates a validated requirement for these skills in the future force structure. This course may become the centerpiece for developing leaders of cyber warfare.

Personnel

Previous sections have discussed the organization, the training, and the leaders involved in the cyber effort within a Brigade Combat Team. This section avoids repeating those discussions, yet intends to critique the quantities from a troop-to-task perspective in order to determine if the right population densities of personnel (by MOS) exist to counter this threat. From the protect or defend perspective, the Signal proponent has sufficiently populated the Brigade headquarters and associated command posts. Transitioning to a support or exploitation role, the Intelligence proponent reflects a priority towards analysis. Since cyber is not one of the four major forms of intelligence (SIGINT, HUMINT, IMINT, MASINT) it is unlikely to command attention from an all-source analyst. A lack of representation by the Fires proponent clarifies the view that the

attack functionality is considered non-lethal. Accordingly, the assignment of an Electronic Warfare Officer and targeting NCOs within the Information Operations Section signifies the potential role for offensive cyber operations in a Brigade Combat Team.

Summary

The modified DOTMLPF analysis qualified the preparedness of Divisions and Brigade Combat Teams to operate in cyberspace and execute cyber warfare. Whereas the initial research answered the question of "what" by identifying the existence of the cyber threat, the DOTMLPF analysis answered the "so what" question regarding what has been done to prepare for this new environment and potential threat. Unfortunately, it revealed a lack of guidance in the form of doctrine which causes cascading deficiencies for the remaining DOTMLPF components. Answering this second question was the final step in responding to the primary research question, "Is the Army ready for cyber warfare at the tactical level of operations?" The preceding analysis indicates the Army is not ready for cyber warfare at the tactical level because it fails to characterize both responsibility and authority for cyberspace. This finding will be discussed further in the next chapter.

This chapter presented analysis using the accepted construct: the primary question was broken down by the two secondary questions, and those secondary questions further detailed by tertiary questions. The next chapter will relate to the primary research question by drawing conclusions and offering recommendations. It will explain what the answers mean. It will discuss what this entails for the force and to future operations. It will draw conclusions from the entire analysis and suggest recommendations for the way ahead. Additionally, suggested areas for further research will be offered.

CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

> Knowledge must become capability.
>
> — Carl von Clausewitz, *On War (1832)*

> The capabilities to move information not only around the battlefield but also around the world have grown exponentially, IO's importance grows daily, and our enemy, who recognizes that victory can be secured in this domain alone, has seized the opportunity to be the best at operating in the information domain. We must learn to employ aggressive IO. We cannot leave this domain for the enemy; we must fight him on this battlefield and defeat him there just as we've proven we can on conventional battlefields.
>
> — LTG Thomas Metz, *Massing Effects in the Information Domain (2006)*

> Since computer network operations and EW are exclusively conducted through "the use of electronics and the electromagnetic spectrum," there is an overlap between IO activities and what our national strategy defines as military capabilities in the cyberspace domain (that is, cyber warfare).
>
> — LTG Keith Alexander, *Warfighting in Cyberspace (2007)*

The primary research question of this study asked this, "Is the Army ready for cyber warfare at the tactical level of operations?" This chapter relates to the research question by drawing conclusions from this finding and offering recommendations for the way ahead. It will explain what the answers are, why they are important, what they mean to today's leaders, and what decisions must be made. The previous chapter presented analysis using the accepted construct: the primary question was broken down by the two secondary questions, and those secondary questions further detailed by tertiary questions. With the primary research question answered, this chapter will discuss what this entails for the force and to future operations through concluding thoughts and by suggesting recommendations as an expression of DOTMLPF- the Army's model for managing change. Finally, suggested areas for further research will be offered.

Conclusion

As previously discussed in chapter 4, the Army is not ready for cyber warfare at the tactical level of operations. The problem lies in the characterization of both responsibility and authority for cyberspace. First, and foremost, the existing body of doctrine does not adequately address it as a capability. The doctrine is not current with the technologies in use by the force, and more importantly, not relevant in regards to the current operational environment. It is analogous to beginning a journey without knowing the destination. Subsequently, the guidance for how a unit's organizations would utilize cyber warfare as an aspect of existing staff proponents or warfighting functions is deficient. The inability to align cyber functions within the modular force organizational structure is similar to beginning the journey without a map. The lack of such guidance further limits the ability of specific branches or functional areas to ensure the right personnel are present in the organization. It also challenges their ability to articulate training requirements for personnel, which prevents them from assigning proficient soldiers to execute the mission. Without understanding who needs to be on this journey, one cannot prepare participants for obstacles which lay ahead. Finally, absent of an understanding for the required skillsets of individual soldiers, a void in leader education is unavoidable. The journey has begun, but no one is in charge.

Reflecting upon Kasserine Pass, the creation of a separate Armored Force was the culmination of the U.S. Army's interwar period and recognition that warfare was once again upon us. Understanding that there was only so much that could be accomplished in the limited time available, Marshall acknowledged that "military operations abroad constitute a great laboratory and proving ground for the development and testing of

organization and materiel" (Marshall 1941, 1). This was a painful reality for the soldiers of Kasserine Pass who died struggling to implement this innovation against a better prepared foe. It is also a premise echoed in the conclusion of *The Dynamics of Military Revolution*, as historians Williamson Murray and MacGregor Knox warn that the U.S. "must always bear in mind the danger that one of America's claimed or covert enemies- rather than America itself- may launch the next revolution in military affairs. And they must understand that if the past is any guide at all, the cost of failure to change now will be a far higher price in lives and treasure to be paid later. For battlefield adaptation- OJT or on-the-job training . . . has always proven exceedingly bloody, costly, and painful" (Knox and Murray 2001, 194). If Armor emerged as the combat arm of decision, now is the time to determine how Cyber can emerge as the information arm of decision.

Information operations are a major theme in today's contemporary operating environment and they drive a cyber requirement at the tactical level. The current force is rapidly embracing technologies as they become available in an effort to enhance the commander's situational understanding and decision making. This is important because doctrine is evolving slower than technology, thus creating an absence of the necessary guide to action that provides a common reference across the force. The absence of doctrine has a cascading effect along the DOTMLPF domains and results in a tactical force not prepared to execute cyber warfare. It means that we have introduced vulnerabilities to the force as they haphazardly enter cyberspace in the presence of adversaries whose intentions are not clearly understood. Therefore our units and their ad hoc approach to this new domain of warfare are at great risk and the Army must act now to avoid www.kasserinepass.com.

Recommendations

One of historian Williamson Murray's conclusions after completing the book, *Military Innovation in the Interwar Period*, is that the institutional processes are absolutely necessary "in the specific sense of linking those inherently imprecise and ever-evolving visions" of future war "to concrete decisions over time about new military systems, operational concepts, doctrines, and organizational arrangements" (Murray and Watts 1996, 410). Therefore recommendations should relate back to our DOTMLPF analysis and suggest direction for each of those respective domains. The observations of Steven Rosen in his book *Winning the Next War* are the guiding principle for all of these recommendations; "Peacetime innovation has been possible when senior military officers . . . reacting not to intelligence about the enemy but to a structural change in the security environment, have acted to create a new promotion pathway for junior officers practicing a new way of war" (Rosen 1991, 127).

Doctrine and Organization

Cyber warfare should be an Information Operations driven activity. This will correlate it to the warfighting function of "command and control," as well as the "information" element of combat power. "While cyberwar is the kind of Internet combat that most worries people, we tend to forget that it's really a subset of Information War" (Dunnigan 2003, 104). To optimize the execution of cyber warfare, operations must be delineated by the three predominant functions of defensive, offensive, and support. Defensive operations are currently referred to as computer network operations and fall under the purview of the Signal Corps. Offensive operations should be delegated to the Fires community in order to align them with existing targeting procedures and the

cognitive staff efforts required to prepare a commander for those decisions. Finally, cyber support operations will be an Intelligence responsibility. The separate aspects of cyber warfare align with existing warfighting functions. Additionally, there is an opportunity to better explore working groups or integrating processes that can form separately to address specific activities in the operation as currently suggested in FM 3-0 (FM 3-0 2008, 5-20).

Characterizing offensive operations as a Fires responsibility offers several advantages. One of which is the opportunity to transition the electronic warfare (EW) subset of electronic attack (EA) to the Fires proponent. This will prevent gray areas arising as adversaries use the electromagnetic spectrum to access cyberspace. Additionally, there are various challenges regarding the legal aspects inherent in cyberspace as well as the electromagnetic spectrum. The Staff Judge Advocate currently advises the commander during targeting and will continue to do so within this new environment. This approach to offensive cyber operations will address the overlap with other Information Operations (IO) functions, while maintaining a singular proponent for both lethal and nonlethal fires.

Cyber support operations can best be accepted by the greater Intelligence community, and indoctrinated by the junior leaders, if a separate intelligence discipline is created. Cyber Intelligence (CYBINT) will parallel the Army's current intelligence disciplines: All-Source Intelligence, Human Intelligence (HUMINT), Imagery Intelligence (IMINT), Signals Intelligence (SIGINT), Measurement and Signatures Intelligence (MASINT), Technical Intelligence (TECHINT), and Counterintelligence (CI) (FM 2-0 2004, 1-30). Though it will begin with intelligence derived from cyber collection methods, it can also mature to the ability to identify an adversary's cyber

capabilities. Such specific intelligence can inform the S6 of what attack capabilities he must be prepared to defend, while identifying potential vulnerabilities our offensive capabilities can attack. More importantly, as an element of all-source analysis, the S2 will instinctively incorporate it in standard products and commanders will expect it. CYBINT can also be the Army's method to address Open-Source Intelligence (OSINT), a joint term describing intelligence derived from unclassified sources- the majority of which are Internet-based. Currently, FM 2-0 defines OSINT as a category of information and integrates it into an all-source analytical approach (FM 2-0 2004, 1-30).

Training and Leader Development

With established proponency, respective branches and functional areas can identify the knowledge, skills, and attributes required of their personnel and articulate the necessary learning objectives to be added to existing curriculum. Additionally, these proponents should visualize learning through the dynamics of expertise, familiarization, and exposure when measuring the delivery of a program of instruction. Personnel must strive to become experts in the duties commensurate with positions at their grade. Personnel should become familiar with the roles and responsibilities of the other proponents, as well as the understanding of how it correlates with their functions. Additionally, personnel should become familiar with the next higher duty position within their proponent and their roles and responsibilities. This will enhance the upcoming relationship once they join the organization, while preparing those who unfortunately are expected to step up to the next echelon due to inadequate manning levels. Finally, personnel could be exposed to the greater realm of cyber warfare and the various future considerations being made by their Directors of Combat Developments. A simple

overview of those efforts will allow them to better prepare for their future, as well as potentially preparing them to recognize changes in the operational environment and posturing them to adjust accordingly. This exposure can also facilitate innovative thinking within the force, as soldiers can glimpse into the future and give consideration to what is ahead for them.

The overall cyber warfare responsibility at the tactical level will need to reside in the Information Operations Staff Officer. Though recommendations have been made for the Brigade FSO, S2, and S6 to lead the separate functions of offensive, support, and defensive cyber operations- a single staff officer needs to facilitate a comprehensive approach for the commander's engagement within the information environment. It also offers a "checks and balances" opportunity through oversight of activities that represent only a fraction of the peer staff sections' responsibilities. It will also facilitate crosstalk; as the S2 discusses CYBINT revelations regarding the weaknesses of an adversary's computer operating systems--the S6 will be asked if we utilize the same operating systems and if we have addressed these vulnerabilities. The software market place is a global entity and the majority of nations incorporate some version of Microsoft or Linux into their daily computing. Whether or not this "lead" role for cyber warfare indicates actual personnel authorizations within that staff section is premature; however, it does suggest the need for the Information Operations Officer to be a multifunctional MOS where the individual previously served in one of those particular specialties.

Regarding Leader Development, FA30, Information Operations, needs to become a multi-functional occupational category--similar to a Multi-functional Logistician (FA90). In the FA90 example, at the transition from company to field-grade officer, the

Transportation (FA88), Ordnance (FA89), and Quartermaster (FA92) branches feed into FA90. Using this approach, company-grade officers serving in Civil Affairs (FA38), Public Affairs (FA49), PSYOP (FA37), Electronic Warfare (FA29), and Systems Automation (FA53) feed into FA30 upon the transition to Major. Obviously, either a stand-alone Information Operations course would bring it together for that individual at the point of transition or, the current components of the Information Operations course would need to be incorporated into these separate MOS schoolings.

Personnel

The majority of literature reviewed indicated a significant challenge ahead regarding the incorporation of cyber personnel in the military. "As currently structured the U.S. military has no chance of finding, attracting, or developing the ideal kind of person we need for waging a knowledge war. . . . Our current ethos of egalitarianism, attention to rigid processes, well-defined standards, a hierarchical leadership structure . . . won't meet the requirements we have for developing, nurturing, and retaining the ideal cyber warrior" (Hall 2003, 190). LtCol Gregory Conti and Col John Surdu use specifc examples from the tactical environment to reinforce their opinion that the existing military services are fundamentally incompatible with that of cyber warfare. "It is useful to examine what these services hold dear- skills such as marksmanship, physical strength, and the ability to jump out of airplanes and lead combat units under enemy fire. Accolades are heaped upon those who excel in these areas. Unfortunately, these skills are irrelevant in cyber warfare" (Conti and Surdu 2009, 16). They contend that although each service has created some sort of a cyber component, "these organizations exist as ill-fitting appendages that attempt to operate in inhospitable cultures where technical

expertise is not recognized, cultivated, or completely understood" (Conti and Surdu 2009, 15). This opinion indirectly suggests a possible solution set regarding the personnel that will ultimately fulfill such requirements and overcome this culture gap. Such an incompatibility suggests the Army incorporate a modified version of Marcus Rogers' hacker taxonomy discussed in the previous chapter.

During the recruitment and initial training phases, cyber soldiers should be categorized as either *Novice*/*Cyber Punk* or *Virus Writer/Old Guard Hacker/Information Warrior.* The latter will be assigned at the operational and strategic level, specifically to conduct CYBINT activities in order to determine adversary weakness and then to write the "toolkits" and "rootkits" that exploit those vulnerabilities. The former will be at the tactical level analyzing the CYBINT to recognize the correlation of adversary weaknesses with their known enemy order of battle, then downloading the particular "toolkit" written for that vulnerability. Now armed, they participate in the targeting process and await the commander's decision to execute their cyber attack. This approach makes the assumption that cyber "geeks" at the lower echelon of competency will be more susceptible to the challenges of the combat environment while those experienced "hackers" at the upper echelon of competency can work at the strategic level and be coddled by an environment they find more acceptable. More importantly, the expertise at the strategic level has an avenue (CYBINT) to channel the necessary information and resources to empower cyber soldiers at the tactical level. In doing so, the common warfighting function for threat analysis, "Intelligence," coupled with a standard warfighting function for effects, "Fires," yields the required support to the commander's situational understanding and decision cycle. It is understood that no single staff officer is

designated as the "effects coordinator" and no single staff section or command post cell is assigned responsibility for "effects" (FM 3-90.6 2006, xix).

Suggestions for Further Research

This study alludes that the development of future Information Operations doctrine is key to clarifying the role of cyber warfare and its complement to other competencies within the information environment. It would be beneficial to research the genesis of the Army's 1st Information Operations Command (Land) and its development since originating as the Land Information Warfare Activity (LIWA). Analysis of its MTOE changes over time would provide insight into the doctrinal concepts that influenced unit organization, training, and personnel. Understanding the "lifecycle" may provide a guide to the necessary changes required within our modular force. Additionally, an effort to consolidate the five "Army Information Tasks" would provide additional clarity to this emerging domain. Specifically, "information engagement" as the overall characterization for offensive operations, "information assurance" for defensive operations, and "information exploitation" for support operations.

Additionally, a study into the possible use of FA30, Information Operations, as a multi-functional occupational category can provide insights regarding the personnel and associated training required for future success. For example, at the transition from company to field-grade officer, the Transportation (FA88), Ordnance (FA89), and Quartermaster (FA92) branches feed into a Multi-functional Logistician (FA90). Did that work? What lessons were learned? Is it feasible to have company-grade officers serving in Civil Affairs (FA38), Public Affairs (FA49), PSYOP (FA37), Electronic Warfare (FA29), and Systems Automation (FA53) feed into FA30 upon the transition to Major?

What specific aspects of the current Information Operations course would need to be incorporated in these MOS schoolings in order to set the competency foundation for that eventual Information Operations officer?

Finally, there should be a classified study that explicitly analyzes current and emerging capabilities of our cyber force in order to suggest tactical applications of cyber warfare. For example, the current posture at the BCT is an area defense, where the BCT S6 is "alone and unafraid" defending his network. The lack of CYBINT translates to limited, if any, ISR support to his cyber threat. Security professionals use the term "honeypot" to refer to a system created solely to monitor, detect, and capture security threats against it (Bragg et al. 2004, 799). Can we transition to a mobile defense by employing a "honeypot" and then resourcing the Fires Section with a "hacker" strike force? What are the technical limitations that dictate how enemy proximity will determine the decision to use electronic attack versus of a computer network attack? In a counterinsurgency, does the likely proximity to the population invoke legal restrictions on CYBINT collection efforts? Does a reliance on the population for intelligence compel a military presence on social networking sites? Such a study, concluding with definitive proposals for the modular force, would initiate the necessary DOTMLPF discussions to progress our tactical echelons into cyberspace.

GLOSSARY

command and control warfare--the integrated use of physical attack, electronic warfare, and computer network operations, supported by intelligence, to degrade, destroy, and exploit an enemy's or adversary's command and control system or deny information to it. [FM 3-0]

cyber-electronics in full spectrum operations-- an emerging, comprehensive operational concept that includes the integrated use of Computer Network Operations (CNO), Electronic Warfare (EW), Electromagnetic Spectrum Operations (EMSO), Space Superiority (SS), Network Operations (NetOps), and Network Warfare (NetWar) in order to achieve effects in and through cyberspace and across the broader Electromagnetic Spectrum (EMS). [USACEWP]

cyberspace--hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. [NSSC, 2003]

cyber warfare--units organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means. The primary difference between cyber terrorism and cyber warfare lies in the condition of the actor, whether or not the actor is state, non-state, or sub-state. [Billo and Chang, 2004]

information management--the science of using procedures and information systems to collect, process, disseminate, or act on information. [FM 3-0]

information operations--the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decisionmaking while protecting our own. [FM 3-0]

information protection--active or passive measures that protect and defend friendly information and information systems to ensure timely, accurate, and relevant friendly information. It denies enemies, adversaries, and others the opportunity to exploit friendly information and information systems for their own purposes. [FM 3-0]

information superiority-- the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. [FM 3-0]

REFERENCE LIST

Alexander, Keith B. 2007. Warfighting in cyberspace. *Joint Forces Quarterly*. Issue 46, (31 July 2007). http://www.ndu.edu/inss/Press/jfq_pages/editions/i46/12.pdf (accessed on September 7, 2008).

Arquilla, John and David Ronfeldt. 1997. *In Athena's camp: Preparing for conflict in the information age.* Washington, DC: Rand Corporation.

Atkinson, Rick. 2002. *An Army at dawn.* New York: Henry Holt and Company, LLC.

Berkowitz, Bruce. 2003. *The new face of war: How war will be fought in the 21st Century*. New York: The Free Press.

Bielakowski, Alexander M. 2002. Mechanization in the Interwar U.S. Cavalry. In *U.S. Army Cavalry officers and the issue of mechanization, 1916-1940*. PhD diss.: Kansas State University.

Billo, Charles and Welton Chang. 2004. *Cyber warfare: An analysis of the means and motivations of selected nation-states.* Institute for Security Technology Studies at Dartmouth College.

Blane, John V. 2003. *Cybercrime and cyberterrorism: current issues.* Hauppauge, NY: Novinka Books.

Blumenson, Martin. 1986. Kasserine Pass, 30 January-22 February 1943. In *America's first battles, 1776-1965*. Edited by Charles E. Heller and William A. Stofft, 226-265. Lawrence, KS: University Press of Kansas.

Bragg, Roberta, Mark Rhodes-Ousley, and Keith Strassberg. 2004. *Network security, The complete reference.* New York: McGraw-Hill / Osborne.

Brown, Bobby. 2006a. *Battalion S6 Officer program of iInstruction.* Fort Gordon, GA: United States Army Signal Center and Fort Gordon.

———. 2006b. *Signal captain's career course program of instruction.* Fort Gordon, GA: United States Army Signal Center and Fort Gordon.

Cammons, Dave, John B. Tisserand III, Duane E. Williams, Alan Seise, and Doug Lindsay. 2008. *U.S. V Corps and 3rd Infantry Division (Mechanized) during Operation Iraqi Freedom combat operations (March to April 2003) Volume I: Operations.* Carlisle Barracks, PA: Center for Strategic Leadership.

Clausewitz, Carl von. 1976. *On war*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press.

Conti, Gregory and John “Buck” Surdu. 2009. Army, Navy, Air Force, and cyber--is it time for a cyberwarfare branch of military? *IAnewsletter* 12, no. 1 (Spring 2009): 14-18. http://www.rumint.org/gregconti/publications/2009_IAN_12-1_conti-surdu.pdf (accessed on March 14, 2009).

Dunnigan, James F. 2003. *The next war zone: Confronting the global threat of cyberterrorism.* New York, NY: Citadel.

England, Robert. 2008. *Action memo: Definition of cyberspace.* Washington, DC: Department of Defense. September 29.

Funk, William. 2008. Army Operational Electronic Warfare Cource (AOEWC). *Field Artillery CSM newsletter, REDLEG-7* (July): 15.

Gates, Robert M. 2008. *National defense strategy.* Washington, DC: United States Government.

Gaudin, Sharon and Larry Greenemeier. 2007. Cyber warfare: A realistic appraisal. *Information Week* (4 June): 49- 50. Accessed from the ABI/Inform database.

Hall, Wayne Michael. 2003. *Stray voltage; War in the information age*. Annapolis, MD: Naval Institute Press.

Heller, Charles E., and William A. Stofft. 1986. *America's first battles, 1776-1965.* Lawrence, KS: Univesity Press of Kansas.

Henderson, Scott J. 2007. *The dark visitor.* Fort Leavenworth, KS: Foreign Military Studies Office (FMSO).

Hildreth, Steven. 2001. Cyber warfare. In *Cyber warfare: Terror at a click,* by John V. Blane, 1-22. Huntington, NY: Novinka Books.

House, Jonathan M. 1984. *Toward combined arms warfare: A survey of 20th-Century tactics, doctrine, and organization.* Fort Leavenworth, KS: Combat Studies Institute Press.

Knox, MacGregor and Williamson Murray. 2001. The future behind us. In *The dynamics of military revolution, 1300-2050*. Edited by MacGregor Knox and Williamson Murray, 175-194. New York: Cambridge University Press.

Kruse II, Warren G., and Jay G. Heiser. 2002. *Computer forensics, Incident response essentials*. New York: Addison Wesley.

Kulifay, Bernard. 2002. *251A WOBC program of instruction.* Fort Gordon, GA: United States Army Signal Center and Fort Gordon.

Libicki, Martin C. 2007. *Conquest in cyberspace: National security and information warfare.* New York, NY: Rand Corporation.

Marsan, Carolyn D. 2007. How close is World War 3.0? Examining the reality of cyberwar in wake of Estonian attacks. *Network World* 24, no. 33 (27 August): 1, 22, 24-25. http://www.networkworld.com/news/2007/082207-cyberwar.html?t51hb (accessed October 19, 2008).

Marshall, George C. 1941. Biennial report of the Chief of Staff of the U.S. Army July 1, 1939, to June 30, 1941 to the Secretary of War. Washington, DC (1 July).

McClure, Stuart, Joel Scambray, and George Kurtz. 1999. *Hacking exposed; Network security secrets & solutions*. New York: Osborne / McGraw-Hill.

Metz, T. F., M. W.Garrett, J. E. Hutton, & T. W. Bush, 2006. Massing effects in the information domain: A case study in aggressive information operations. *Military Review* (May/June): 103-113.

Moteff, John D. 2001. Critical Infrastructures: Background and Early Implementation of PDD-63. In *Cyber warfare: Terror at a click*, by John V. Blane, 47-76. Huntington, NY: Novinka Books.

Murray, Williamson. 1995. The World in Conflict 1919-1941. In *Cambridge illustrated history of warfare*. Edited by Geoffrey Parker, 298-319. Cambridge: Cambridge University Press.

Murray, Williamson A., and Allan R. Millett. 1996. Armored Warfare: The British, French, and German Experiences. In *Military innovation in the interwar period*, 6-49. Cambridge, UK: Cambridge University Press.

Murray, Williamson A., and Barry Watts. 1996. Military innovation in peacetime. In *Military innovation in the interwar period*, 369-415. Cambridge, UK: Cambridge University Press.

Myers, Richard. 2004. *National military strategy.* Washington, DC: Department of Defense.

Norton-Taylor, Richard. 2007. Titan Rain- how Chinese hackers targeted Whitehall. *Guardian* (September 4). http://www.guardian.co.uk/technology/2007/sep/04/

news.internet (accessed October 19, 2008).

Radice, Richard. 2007. "Dominating cyberspace." Strategy Research Project, United States Army War College, Carlisle Barracks, PA.

Robb, John. 2007. *Brave new war.* Hoboken, New Jersey: John Wiley & Sons, Inc.

Rogers, Marcus K. 2005. *The development of a meaningful hacker taxonomy: A two-dimensional approach.* Unpublished paper, Purdue University, West Lafayette, Indiana.

Rosen, Stephen Peter. 1991. *Winning the next war: Innovation and the modern military*. Ithaca: Cornell University Press.

Shachtman, Noah. 2008. Georgia under online assault. *Wired.com* (August 10). http://www.wired.com/dangerroom/2008/08/georgia-under-o (accessed October 19, 2008).

Shy, John. 1986. First battles in retrospect. In *America's first battles, 1776-1965*, by Charles E. Heller and William A. Stofft, 327-352. Lawrence, KS: University Press of Kansas.

Smith, Francis W. 2008. 35G critical task list. Fort Huahchuca, AZ: United States Army Intelligence Center and Fort Huahchuca.

Sorkin, Michael. 2008. *Indefensible space: the architecture of the national insecurity state.* New York: Routledge, Taylor & Francis Group.

Thomas, Timothy L. 2005. *Cyber silhouettes: Shadows over information operations.* Fort Leavenworth, KS: Foreign Military Studies Office.

Turabian, Kate L. 1996. *A manual for writers.* 6th ed. Chicago: University of Chicago Press.

United States Army. 2005. FM 1-0, *The Army*. Washington, DC: U.S. Government Printing Office (April).

———. 2004. FM 2-0, *Intelligence*. Washington, DC: U.S. Government Printing Office (May).

———. 2008. FM 3-0, *Operations*. Washington, DC: U.S. Government Printing Office (February).

———. 2003. FM 3-13, *Information operations: Doctrine, tactics, techniques, and procedures*. Washington, DC: U.S. Government Printing Office (November).

———. 2009. FM 3-36, *Electronic warfare: Doctrine, tactics, techniques, and procedures*. Washington, DC: U.S. Government Printing Office (February).

———. 2006. FM 3-90.6, *The brigade combat team*. Washington, DC: U.S. Government Printing Office (August).

———. 2004. STP No. 6-13F14-SM-TG PROPO*, Soldier's manual and trainer's guide: MOS 13F*. Washington, DC: U.S. Government Printing Office (October).

———. 2008. TRADOC Pamphlet 525-5-500, *Commander's appreciation and campaign design*. Washington, DC: U.S. Government Printing Office (January).

United States Army Combined Arms Center Blog. *Army-Marine Corps collaborate to 'attack the network'*. http://usacac.leavenworth.army.mil/BLOG/blogs/cdid/archive/2009/03/16/army-marine-corps-collaborate-to-attack-the-network.aspx (accessed March 16, 2009).

United States Army Signal Center of Excellence. 2008. *Campaign plan, 500-day plan: March 2008-July 2009.* Fort Gordon, GA.

United States Department of Defense. 2007. JP 1-0, *Doctrine for the Armed Forces of the United States.* Washington, DC: Government Printing Office (May).

———. 2008. JP 3-0, *Joint operations.* Washington, DC: Government Printing Office (February).

———.. 2007. JP 3-13, *Information operations.* Washington, DC: Government Printing Office (May).

United States Department of Defense CIO. 2007. *Department of Defense global information grid architectural vision: Vision for a net-centric, service-oriented DoD enterprise.* Washington, DC: Government Printing Office (June).

United States Government. 2003. *The national strategy to secure cyberspace.* Washington, DC: Government Printing Office.

Verton, Dan. 2003. *Black Ice: The invisible threat of cyber-terrorism.* New York, NY: McGraw-Hill Osborne Media.

White, Thomas E. 2002. *Headquarters, Department of the Army General Orders No. 5.* Washington, DC: Government Printing Office (13 August).

Zi, Sun. 2003. *Art of war.* Translated by Chow-Hou Wee. Singapore: Prentice Hall.

INITIAL DISTRIBUTION LIST

Combined Arms Research Library
U.S. Army Command and General Staff College
250 Gibbon Ave.
Fort Leavenworth, KS 66027-2314

Defense Technical Information Center/OCA
825 John J. Kingman Rd., Suite 944
Fort Belvoir, VA 22060-6218

Dr. Jack Kem
DJIMO
USACGSC
100 Stimson Ave.
Fort Leavenworth, KS 66027-1352

Mr. Brian Blew
CTAC
USACGSC
100 Stimson Ave.
Fort Leavenworth, KS 66027-1352

LTC John E. Bircher, IV
U.S. Central Command, ATTN: CCPA
7115 South Boundary Blvd
MacDill AFB, FL 33651-5101

Director, CAC-CDID
USACAC
806 Harrison Drive
Fort Leavenworth, KS 66027-2326