United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

APPLICATION OF US SPECIAL OPERATIONS COMMAND MODEL TO DEPARTMENT OF DEFENSE CYBERSPACE FORCE

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTERS OF MILITARY STUDIES

LIEUTENANT COLONEL BRADLEY L. PYBURN

AY 08-09

Mentor and Oral Defense Committee Member: Douglas G. Strecosper
Approved:
Date: 8 April 2009

Oral Defense Committee Member: Paul D. Gelpi, Jr.
Approved:
Date: 8 April 2009

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Application of US Special Operations Command Model to Department of Defense Cyberspace Force	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **United States Marine Corps,Command and Staff College, Marine Corps Combat Dev,Marine Corps University, 2076 South Street,Quantico,VA,22134-5068**	8. PERFORMING ORGANIZATION 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 unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**30**	

Executive Summary

Title: Application of US Special Operations Command Model To Department Of Defense Cyberspace Force

Author: Lt Colonel Bradley L. Pyburn, United States Air Force

Thesis: The US Special Operations Command structure, with its unique coupling of combatant command authority and service-like responsibilities, provides a viable model for establishing a professional DoD cyberspace force and organization.

Discussion: The potential for operations in cyberspace is only matched by the vulnerabilities it creates to our national defense. US critical infrastructures depend on freedom of action in cyberspace to provide essential services to our citizenry. Within the DoD, service-centric cyber force development, an ineffective cyber organizational structure, weak C2 of cyber forces, and limited oversight of cyber technology and personnel development hinders our ability to defend US interests in cyberspace. As a result, the DoD must make significant organizational, personnel, and doctrinal changes to ensure our continued superiority in the cyber domain. The USSOCOM structure provides a viable option for organizing, equipping, and leading cyber forces.

Conclusion: The USSOCOM model provides significant advantages for cyberspace organizational structure, cyber personnel management, cyber weapons and systems development, and cyberspace doctrine. Establishing a sub-unified command for cyberspace under the purview of USSTRATCOM is a promising option.

Table of Contents

Disclaimer

The opinions and conclusions expressed herein are those of the individual student author and do not necessarily represent the views of either the Marine Corps Command and Staff College or any other government agency. References to this study should include the foregoing statement.

Preface

The following thesis is a result of my career experience as an Air Force communications and information officer, and specifically my previous assignment at Joint Task Force – Global Network Operations, US Strategic Command, from August 2005 to June 2008. This study, along with its recommendations, would not have been possible without the continued support of two groups: my peers who continue to defend US interests in cyberspace and many of my superiors who serve as a springboard for new ideas. I'd like to especially thank Brigadier General Jennifer Napper, Colonel Gary McAlum, Colonel Barry Hensley, and Colonel Stephen Korns for their guidance, mentorship and support. Additionally, I'd like to thank Lieutenant Colonel Dave Burton, Dr. Doug Streusand, and Dr. Donald Bittner – members of the outstanding faculty of the Marine Corps Command & Staff College – whose superb tutelage shaped the critical thinking that drove the analysis behind this study.

Background

Cyberspace, the newest warfighting domain, offers tremendous promise as the US government and commercial industry continue the move towards cyber-centric operations. The incredible potential of operating in cyberspace also creates significant vulnerabilities and challenges. The cyber attack against Estonia in April 2007 highlights both the ease with which a determined foe can cripple cyber networks and the far-reaching impacts on the victim. The need to protect and defend US cyberspace reached a fever pitch in January 2008 when the President directed an interagency group, including the Department of Defense (DoD) and Department of Homeland Security (DHS), to address the issue. During the same period, each of the military services – most notably the US Air Force – developed some measure of cyberspace doctrine, organization, and personnel management plans. Along with the challenges of service-dependent cyberspace development, the current DoD cyberspace organizational structure inhibits effective command and control (C2) of cyber forces and does little to provide oversight for cyber weapons, systems, and personnel development. Clearly, some change is needed to effectively organize, equip, and lead cyber forces in the defense of our nation's critical infrastructures. The US Special Operations Command (USSOCOM) structure, with its unique coupling of combatant command authority and service-like responsibilities, provides a viable model for establishing a professional DoD cyberspace force and organization. This paper – after providing some background on current cyberspace development and organization, plus a primer on USSOCOM – analyzes the applicability of the USSOCOM model to developing a professional DoD cyberspace force and organizational construct.

Definition of Cyberspace

As the DoD struggled over the last several years to organize and fight in cyberspace, the US government refined the definition of cyberspace through the efforts of several agencies and working groups. In 2003, the White House released *The National Strategy to Secure Cyberspace*, which defined cyberspace as "the nervous system of these [critical] infrastructures – the control system of our country. Cyberspace comprises hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables …essential to our economy and national security."[1] In September 2006, the Joint Chiefs of Staff developed a broader definition, which described cyberspace as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."[2] The Joint Chiefs of Staff definition, by including the electromagnetic spectrum, threatened to stall DoD efforts by dramatically increasing the scope of the cyberspace domain. Subsequently, during the development of *National Security Presidential Directive 54/Homeland Security Presidential Directive 23* (a classified document) in late 2007, a team of interagency experts developed a more narrow unclassified definition, describing cyberspace as a "network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Leveraging the interagency group's efforts, Deputy Defense Secretary Gordon England refined the DoD definition in May of 2008 by defining 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."[3]

Utilizing the most current definition, DoD is postured to organize, train, and equip the forces to defend US interests in the cyber domain.

Air Force Cyberspace Forces

In April of 2008, the Air Force developed a roadmap to organize, train, and equip cyberspace forces in accordance with an updated mission to extend global reach, power, and vigilance into the cyber domain. Fundamental to the Air Force development of cyberspace professionals is the Air Force concept of operations in the cyber domain. Air Force actions in cyberspace consist of cyberspace operations, cyberspace cross-domain operations, cyberspace combat sustainment operations, and cyberspace intelligence, surveillance, and reconnaissance (ISR). Cyberspace operations provide friendly forces freedom of action in cyberspace while denying the enemy's ability to do the same. Cyberspace operations consist of offensive actions to deny, degrade, disrupt, or destroy, and defensive actions to preserve, protect, recover, and reconstitute. Cyberspace cross-domain operations seek to leverage cyber-unique capabilities to achieve effects in non-cyber domains. For example, cross-domain operations may utilize cyber network attack to defeat enemy air defense systems or degrade enemy C2 systems. Cyberspace combat sustainment will develop and maintain the necessary infrastructure, systems, weapons, and forces to achieve and maintain cyber superiority. Cyberspace ISR provides collection, processing, analysis, and distribution of intelligence for operations in cyberspace. Utilizing the above tenets of cyberspace operations, the Air Force will provide combatant commanders with the ability achieve and maintain cyberspace superiority.[4]

Air Force Cyberspace Core and Enabling Competencies

In addition to the concept of operations for cyberspace, the Air Force outlined the necessary core and enabling competencies for cyberspace forces. The Air Force core competencies for cyberspace include establishing the domain, controlling the domain, and leveraging the domain. Establishing the domain consists of the necessary actions to network electronic devices together for the purpose of exchanging, storing, or modifying information. Air Force personnel control the domain through robust situational awareness, effective battlespace preparation, strong defensive capabilities, and positive command and control (C2) of cyberspace warfare systems. After establishing the domain and implementing control, airmen can leverage the domain at a time and place of their choosing to achieve operational objectives. Leveraging the domain includes offensive actions such as the disruption of sensors and C2 systems, degradation of decision support tools and weapon systems, and manipulation of data. Along with the core competencies, the Air Force outlined intelligence, engineering and acquisition, research, and space operations as enabling competencies. Effective intelligence provides the commander with the situational awareness necessary to operate across all domains – air, space, and cyberspace. The blistering pace of technological development and the Air Force dependence on commercial infrastructures demand a rapid, agile, and streamlined engineering and acquisition process. Coupled with acquisition, cutting-edge research will deliver timely developments to the war fighter, enabling cyberspace superiority. Finally, space operations, such as satellite communications, provide the ability to deliver non-kinetic effects worldwide.[5]

Air Force Cyberspace Career Fields

Using the concept of operations for cyberspace, coupled with the core and enabling competencies, the Air Force defined four primary career fields for cyberspace personnel:

cyberspace operators, cyberspace specialists, cyberspace analysts, and cyberspace developers. Cyberspace operators will plan, direct, and execute cyberspace missions. At the tactical level, cyberspace operators will leverage their technological knowledge to employ cyberspace weapons and systems. At the operational level, cyberspace operators will use their broad knowledge of cyberspace capabilities to plan and shape campaigns to achieve strategic objectives. Cyberspace specialists provide, sustain, and maintain infrastructures and systems supporting cyberspace operations. From maintaining a local area network to installing a server on an airborne platform, cyberspace specialists will perform defensive functions intended to enable operations. Similar to current intelligence analysts, cyberspace analysts will investigate and analyze all possible intelligence sources to provide assessments, indications, and warnings. However, cyberspace analysts must possess additional technological skills, including networking, operating systems, and software. These additional skills provide analysts the tools required to target adversary networks and recognize enemy vectors and technologies for defensive purposes. Cyberspace developers will design and develop tools, weapon systems, and tactics in support of cyberspace operations. Many developers will require advanced academic degrees and in-depth knowledge of hardware and software technology.[6]

The Air Force will populate these new positions from related career fields, across the total force construct of active duty, guard and reserve, civilian, and contractor personnel. The Air Force vision consists of transforming existing officer and enlisted career fields to the cyber-specific career fields described earlier. The new cyberspace career fields will encompass a member's entire career – from accession to retirement – with diverse opportunities across the tactical and operational levels of war. The enlisted force will provide technical depth and technological expertise. The Air Force will transform the existing enlisted communications-

electronics systems, information management, and communication-computer systems career fields into a single cyberspace operations career field consisting of several new Air Force specialties. The officer corps will provide leadership, advocacy, and vision for future cyberspace operations. The foundation of the cyberspace officer corps is the Cyberspace Warfare Officer (CWO), which consists of several variants from the rated and non-rated career fields. Navigators and electronic warfare officers will become rated CWOs, and communication officers will become non-rated CWOs. Ultimately, these variants will be integrated into a single Air Force specialty by 2018. The Air Force will develop the civilian cyberspace workforce alongside the enlisted and officer components. Civilians will choose between a technical and leadership track, maximizing their personal potential while satisfying Air Force requirements. Enlisted, officer, and civilians will attend rank-appropriate cyberspace training and education opportunities throughout their careers.[7]

Army Cyberspace Forces

In April of 2008, the Chief of Staff of the Army directed an assessment of Army cyberspace capabilities and workforce. The assessment team highlighted that Army signal and intelligence branches were providing current Army cyberspace capabilities. The Army's current batch of computer network defenders develop from the signals corps branch, while computer network exploiters and attackers develop from the intelligence branch. The assessment team further determined that the Army's cyberspace equivalent officer corps consists of functional area specialties in information systems engineering and information systems management. While the assessment described a solid foundation of capable personnel, it also clearly demonstrated the need for a professional cyberspace career field.[8]

Following the assessment in the summer of 2008, the Army signals and intelligence branch leadership held a series of meetings to develop options to grow an Army cyberspace career field. Army leadership tasked this group with developing a strategy that facilitated recruitment and retention, maintained a high level of technical skills, provided workforce stability, minimized risk, and most important, was affordable. This group, leveraging Air Force cyberspace concepts, developed recommendations for several new Army cyberspace career fields: cyber planner, cyber engineer, cyber operator, cyber analyst, and cyber developer. The most significant shortfall was the lack of an existing Army career specialty or functional area for cyber operators and cyber planners. To alleviate this and other shortfalls, the group developed several courses of action for the development of an Army cyberspace career field.[9]

The potential courses of action consisted of the mid-career accession model, initial entry model, career management field (CMF) model, cyber tech model, and additional skills identifier (ASI) model. The mid-career accession model would be open to all Army specialties, but would target those soldiers with signals intelligence or information technology expertise. Enlisted soldiers would morph into enlisted or warrant officer cyber operators, cyber analysts, computer network attack and exploitation technicians, and computer network defense operators. Officers would transfer to a new functional area for cyber operations, planning, and synchronization. In the initial entry model, cyberspace aptitude and pre-military education and training would determine placement. Soldiers would attend core cyberspace training, and further assessment and needs of the Army would determine the specific cyberspace career path. The most costly option is the CMF model. In the CMF model, the new cyberspace career field would consume parts of military intelligence and signals intelligence, all of the signal corps branch, and all future electronic warfare specialties. The cyber tech model would create a new warrant officer

specialty that performs all Army cyberspace operations functions. The Army would primarily target the military intelligence and signal corps specialties for the cyber tech model, but other specialties would be allowed to join based on aptitude. The cheapest and least disruptive to implement is the ASI model. In the ASI model, the Army would develop ASIs for certain cyberspace skills, incorporate high-end cyberspace skills into the Great Skills program, and require no change to existing Army specialties. While the information obtained for this paper on Army cyberspace career field development was pre-decisional, the ASI model exhibited the best course of action analysis score.[10]

Navy Cyberspace Forces

As the executive agent for Computer Network Operations (CNO) in DoD, Navy operations in cyberspace are heavily rooted in the doctrine of CNO. To meet the growing threat in cyberspace and better posture the force for CNO, the Navy established the Cryptologic Technician Networks (CTN) rating for its enlisted force in February 2004. According to the Navy, the establishment of a single rating for the CNO skill set will allow the force to efficiently and effectively operate in cyberspace. The Navy develops CTNs through a series of digital network analysis and network attack education courses at the apprentice, journeyman, and master levels. As a CTN matures in rank, they will experience a number of diverse career opportunities in computer network defense, computer network attack, and computer network exploitation. While the Navy has taken significant actions to prepare its enlisted force for cyberspace operations, they currently have no specific plans to create a cyberspace officer career track.

Marine Corps Cyberspace Forces

In conjunction with the Navy, the Marine Corps continues to develop its cyberspace forces using CNO as the foundation. Through an organization known as Company L, Marine Cryptologic Support Battalion, at Fort Meade, Maryland, the Marine Corps provides deployed units the capability to perform signals intelligence and digital network intrusion analysis. While not planning to develop a specific cyberspace Military Operational Specialty (MOS), the Marine Corps utilizes the 2611 MOS to meet the growing demand for cyberspace expertise. The Marine Corps sources its cyberspace positions through a rigorous screening process, followed by a series of digital network analysis classes provided by the National Cryptologic School and commercial vendors. In addition, Company L provides a variety of training opportunities, including cyber analysis, red teaming, and network operations. In the near future, Company L plans to develop network exploitation, vulnerability analysis, and network attack training programs. Future Marine Corps organizational enhancements include the creation of a Network Warfare Platoon within Company L to augment Joint Force Component Command – Network Warfare (JFCC-NW) operations.[11]

DoD Cyberspace Organization

DoD leadership designated US Strategic Command (USSTRATCOM) with the global mission to ensure US freedom of action in cyberspace and to deliver integrated kinetic and non-kinetic effects in support of Joint Force Commander (JFC) operations. Based on this mission designation, USSTRATCOM is the lead DoD component for cyberspace defense and attack operations. To efficiently accomplish its cyberspace missions, USSTRATCOM delegated day-to-day planning and execution authority for both cyber defense and attack operations to several of its Joint Functional Component Commands (JFCC). The Joint Task Force – Global Network

Operations (JTF-GNO) directs the operation and defense of the Global Information Grid (GIG) to assure timely and secure Net-Centric capabilities across strategic, operational, and tactical boundaries in support of DoD full spectrum warfighting, intelligence, and business missions. In this role, JTF-GNO is responsible for planning and directing cyber defensive actions for all DoD components, including the Services, Combatant Commands, and Defense Agencies. The JFCC-NW plans, and when directed, executes operations in and through cyberspace to assure US and allied freedom of action, denying adversaries' freedom of action, and enabling effects beyond the cyber domain. In this role, JFCC-NW executes offensive cyber operations in support of JFC operations. Finally, the Joint Information Operations Warfare Command (JIOWC) plans, integrates, and synchronizes information operations in direct support of JFC operations and serves as the USSTRATCOM lead for enhancing information operations across the DoD.[12]

In June 2004, the Secretary of Defense designated the Director of the Defense Information Systems Agency as the commander of JTF-GNO. This designation, coupled with the Unified Command Plan 2002 (Change 2), invested in JTF-GNO the authority to direct operations and defense in cyberspace across the GIG. To perform this critical mission, DoD allocated various cyberspace forces from among the Services to JTF-GNO under an operational control (OPCON) relationship. The service cyberspace components consist of the following: the Army Global Network Operations and Security Center (AGNOSC) at Fort Belvoir, Virginia; Air Force Network Operations Center (AFNOC) at Barksdale Air Force Base, Louisiana; Marine Corps Network Operations and Security Command (MCNOSC) at Quantico Marine Base, Virginia; and the Navy Cyber Defense Operations Command (NCDOC) in Norfolk, Virginia. Along with the service components, JTF-GNO also exercises OPCON over the DISA Theater NetOps Centers (TNC) within each regional combatant command. For global cyber defense

issues, USTRATCOM serves as the supported command, and through JTF-GNO directs cyber defensive measures across the GIG. For theater-specific cyber defense issues, the combatant command serves as the supported command, and JTF-GNO supports the appropriate combatant command Theater NetOps Control Center (TNCC) or Global NetOps Control Center (GNCC).[13]

USSOCOM Model

In the wake of the failed Desert One hostage rescue attempt, terrorist bombing attack in Lebanon costing 237 Marines their lives, and significant command and control problems during the Grenada invasion, Congressional concern mounted against the DoD and its ability to conduct low-intensity conflict. In response, the DoD created the Joint Special Operations Agency (JSOA) in January 1984. The JSOA did not possess either OPCON or command authority over any Special Operations Forces (SOF), and did very little to improve readiness or capabilities. After witnessing JSOA's inability to shape the future of SOF, Senators Sam Nunn and William Cohen pushed DoD hard to establish a clear organizational focus and chain of command for low-intensity conflict and special operations missions. The pressure from Senators Nunn and Cohen, along with the Goldwater-Nichols Defense Reorganization Act of 1986, led to the formation of a unified combatant command for all SOF. President Ronald Reagan approved the command and the DoD established USSOCOM on 13 April 1987.[14]

USSOCOM's mission is to provide fully capable SOF to defend the United States and its interests, and to plan and synchronize DoD operations against terrorist networks. USSOCOM is a force provider, supplying SOF to JFCs in support of operational objectives. As a functional combatant command, USSOCOM commands all SOF, synchronizes SOF planning, conducts special operations, plans and executes SOF missions, and deploys SOF in accordance with JFC requirements.[15] In contrast to its identity as a combatant command, USSOCOM is unusual in

that it performs like a service with Title 10 responsibilities.[16] These responsibilities include: to organize, train, and equip SOF; to develop strategy, doctrine, and tactics for SOF; to program and budget for SOF technology; to procure SOF-peculiar equipment upgrades; to monitor SOF personnel management and progression; and to ensure conventional force interoperability with SOF.[17] While the services provide a baseline of personnel and equipment to accomplish special operations, USSOCOM ensures service personnel are organized, trained, and equipped appropriately for SOF missions. These missions include direct action, counterterrorism, foreign internal defense, unconventional warfare, special reconnaissance, psychological operations, civil affairs operations, information operations, and counterproliferation of weapons of mass destruction.[18] Through the successful fusion of combatant command authority with service responsibilities, USSOCOM provides SOF clear organizational focus, unity of command, and synchronized effort.

With a large range of capabilities and a broad distribution of personnel skills, SOF are organized differently than conventional forces.[19] While USSOCOM retains the overarching responsibility for SOF, each military service maintains a component designated as SOF. The Army Special Operations Command consists of Army Special Forces, Civil Affairs, Psychological Operations, the Ranger Regiment, and the 160th Aviation Regiment. The Navy Special Warfare Command contributes SEALs and supporting boat units. The Air Force Special Operations Command provides special operations aircraft and pilots, combat controllers, pararescuemen, and special tactics personnel. In addition to the other services, the Marine Corps recently activated Marine Special Operations Command, which is further developing requirements for Marine SOF capabilities and skill sets. Through the service SOF components, USSOCOM exercises its service-like requirements to organize, train, and equip the force. To

exercise its combatant command authority, USSOCOM installed a SOF component within each regional combatant command. These combatant command SOF components retain command authority over their respective SOF personnel and missions, ensuring they support JFC operational objectives. This unique blend of service and combatant command components allows USSOCOM to execute its congressionally mandated mission to command, organize, train, and equip SOF.[20]

SOF personnel are exceptionally trained and highly motivated, exhibiting specialized expertise across a diverse spectrum of military capabilities. The SOF service components select their members from a pool of volunteers based on that service's requirements. Due to the high standards of SOF, selected personnel tend to be seasoned in their craft and senior in rank. In conjunction with service-provided foundational training, USSOCOM and service SOF components provide additional specialized training and instruction to SOF personnel. As a result of the specialized training and elite nature of SOF, they are highly flexible and able to function in a complex, dynamic environment. In contrast to their elite nature, service in SOF historically had the potential to stunt a member's promotion opportunities; however, USSOCOM largely removed this drawback by monitoring the promotions, training, and professional development of SOF personnel. USSOCOM management and oversight of SOF personnel training and career progression ensures SOF remains a capable, agile, globally responsive force with the ability to create strategic battlefield effects.[21]

Application of USSOCOM Model to DoD Cyberspace Forces

As described earlier, each of the military services are developing cyberspace capabilities in accordance with their respective doctrine and requirements without significant oversight or standardization. USSTRATCOM, who has little control over the services and their cyber

doctrine, systems, and personnel development, exerts limited C2 over theater cyber events where another organization can claim primacy. To successfully defend US interests in cyberspace, the DoD must make significant organizational, personnel, and doctrinal changes. Applying the USSOCOM model to create a professional DoD cyberspace force and organization is explored in the remainder of this document through four perspectives: organization, personnel, systems and technology, and doctrine.

Organization

Although the DoD designated USSTRATCOM as the lead operational component for cyber operations, the current organizational structure inhibits effective C2 of cyber forces and frustrates shared situational awareness of cyber events. Currently, USSTRATCOM exercises OPCON over only the service cyber forces, which creates a tenuous relationship with the other combatant commands when dealing with cyber issues. USSTRATCOM, through its partnership with DISA, directs the operations of DISA TNCs within the combatant commands; however, the TNCs function in a purely supporting role to the combatant command with no directive authority. The Network Operations (NetOps) Concept of Operations (CONOPS)[22], a non-standard and non-binding document, codifies the dysfunctional relationship between the combatant command cyber forces through supporting and supported roles based on the type of cyber event. If a combatant command considers a cyber event regional or theater-based, it claims primacy, and requires USSTRATCOM cyber forces to function in a supporting role. Only cyber events of a global nature allow USSTRATCOM clear operational control, and then only at the pleasure of the combatant commands due to the non-binding nature of the NetOps CONOPS. As a result, responses to cyber events may be non-standard, uncoordinated, and ineffective. This relationship also limits shared situational awareness of both cyber forces and

DoD cyberspace, as combatant commands selectively choose which cyber events to report to USSTRATCOM and other combatant commands. Within USSTRATCOM the organizational challenges exist as well; the entities responsible for cyber defense and cyber attack are located in different organizations (JTF-GNO and JFCC-NW). This separation of attack and defense causes friction between the organizations and creates challenges to effective communication and shared situational awareness. If JFCC-NW fails to properly coordinate an offensive cyber action, JTF-GNO can misinterpret the effects and remain unprepared for potential cyber counter actions. Resultantly, the current cyber organizational structure lacks true unity of command and unity of effort.

Applying the USSOCOM model to DoD cyber forces would provide clear organizational focus, along with streamlined C2 and situational awareness. The DoD, by designating a single component as the command authority for all cyber forces and actions, would remove many of the current problems resulting from the NetOps CONOPS and combatant command relationships. Whether events were global or regional in nature, a DoD cyber command would exercise full control over the event and response actions. Following the USSOCOM structure, cyber command would nest operational components within each combatant command. These nested cyber components would allow cyber command to exercise full operational control over all cyber forces and events while supporting JFC objectives, and would streamline cyber event reporting to create improved shared situational awareness in the DoD cyber community. Additionally, cyber command could leverage the service's organizational groundwork – such as the Air Force proposed cyber command structure – in much the same way as USSOCOM utilizes the service SOF components. Finally, merging the cyber attack and defense entities into one unified command would serve as a force multiplier, increasing coordination and communication on

planned cyber actions and subsequent response actions. Employing the USSOCOM structure to cyber forces would create organizational synergy, solidify unity of command and effort, and streamline situational awareness and coordination.

Personnel

In the current organizational construct, USSTRATCOM exerts little control over the services' development of cyber professionals. As described earlier, each of the services have developed some measure of cyber forces and organization. The Air Force – with probably the most advanced development to date – has outlined plans to develop career enlisted, officer, and civilian cyber professionals. The Air Force plan is in sharp contrast to the Navy, which only plans to develop an enlisted cyber specialty, and the Army, which may use only an ASI to identify skills without creating new specialties. While having each service develop its cyber forces independently has some merit, the lack of oversight to ensure standardization of training and career progression, and adequate depth and breadth for DoD cyber forces, could prove disastrous. The lack of centralized management and control over cyber force development creates significant skill and capability gaps, and reduces the effectiveness of USSTRATCOM and its components JFCC-NW and JTF-GNO, who rely on the services to provide cyber personnel. For example, new personnel at JTF-GNO must train and build experiences for up to 18 months – due to the lack of standardized service training and experience – before becoming proficient in their cyber-related duties. Additionally, once those personnel return to their service, no tracking mechanism exists to ensure their cyber experiences and capabilities are properly utilized in future endeavors. To avoid the above dilemmas, the DoD requires a significant change in management and oversight of cyberspace personnel.

The USSOCOM model of centralized oversight and management of personnel would enable the DoD to create, manage, and sustain a professional cyber force. Using the USSOCOM model would allow the DoD to leverage much of the groundwork already developed by the services. According to Brigadier General (BG) Jennifer Napper, former Deputy Commander of JTF-GNO, "There are multiple groups of cyber skills required for operating in cyberspace…intel analysts, planners, operators, engineers, integrators, and possibly others."[23] BG Napper's vision agrees with much of the Air Force planning on cyber personnel career field development. A joint cyber command could provide the necessary oversight to all services to develop and train the necessary personnel, ensuring the proper depth and breadth of expertise in the cyber specialties highlighted by BG Napper. Most importantly, a cyber command would provide joint management of cyber force personnel recruitment, education, and career progression as a separate entity, much like USSOCOM with service SOF forces. According to BG Napper:

> There are several aspects of the SOF model that appeal to me. Military members are recruited from the ranks of their service, meaning they understand their service, are proven at a particular skill, and have the desire to serve for a longer period. Screening eliminates those lacking the mental propensity for the field. Specialty training follows the service-provided foundational training, and personnel are managed separately without returning to their basic branch or skill. While some current models propose an ASI allowing troops to move in and out of cyber, I non-concur. The cyber force should be joint and managed as a separate entity, even if cyber warriors serve at lower echelons within their service.[24]

Additionally, joint personnel management of cyber forces ensures force interoperability – a cyber operator from one service can communicate, integrate, and execute missions with a cyber operator from a sister service. Force interoperability – an attribute currently lacking from forces provided to JTF-GNO and JFCC-NW – will lay the groundwork for full spectrum, joint operations in cyberspace. Finally, much like airpower advocates of the early 20th century, a separate, joint cyber command would foster "cyber-mindedness". A core set of individuals with cyber expertise could develop cyberspace defense and attack theory, fostering necessary cyber

education and technology development.[25] Adopting the USSOCOM model for management of DoD cyberspace forces would ensure proper oversight of recruitment, training, force interoperability, and career progression.

Systems & Technology

Cyber weapon systems and technology are critical enablers in defending US interests in cyberspace. Unfortunately, USSTRATCOM, the Assistant Secretary of Defense for Networks and Information Integration (ASD-NII), DISA, the National Security Agency (NSA), and the services hinder the effective development and procurement of cyber technology through poor coordination, self-serving interests, and lethargic acquisition. The DoD procures a large amount of technology through portfolio management, which capitalizes on funds contributed by the services. In many cases, the owning agency fails to compel the service to submit the necessary funding, hindering acquisition. Service or agency-dependent technology development, or "stove pipe systems", further exacerbate the problem. Poor coordination between the services and agencies cripples interoperability of technology and systems that are lucky enough to survive procurement. As cyber-centric operations progress, interoperability between cyber defense and attack systems becomes critical; poorly developed systems can wreak havoc in cyberspace operations, effectively blocking access to mission essential applications and systems. Additionally, ASD-NII, DISA, and service information technology acquisition specialists focus on providing capability, not developing warfighting functionality for cyber attack and defense. Lacking true centralized oversight, responsibility, and management, cyber systems acquisitions run amuck, driven by program manager's egos instead of warfighter requirements. In cases where agencies or services are addressing warfighter requirements, the acquisition cycle takes years, missing the ever-shrinking window of opportunity. Much like the SOF forces in the 1970s

and 1980s, USSTRATCOM and its cyber components are headed for a major catastrophe due to the lack of interoperable, capable cyberspace systems and technology.

By designating a single entity be responsible for cyber systems programming and budgeting, and procuring cyber-specific technology, the DoD can provide the necessary oversight and coordination to cyber weapon and systems development. A joint cyber command, with responsibilities similar to USSOCOM for SOF technology, can integrate and synchronize cyber weapons and technology efforts across the DoD and supporting agencies. Cyber command's acquisition processes would eliminate pork barrel projects, shifting the focus to only those most important cyber requirements. Further, following USSOCOM's model, the DoD can establish a streamlined acquisition process, fostering a quick turn on technology development to counter the most devastating cyber threats. By capitalizing on the lessons learned from SOF in the 1970s and 1980s, DoD can avoid the equivalent of a cyber-Grenada or Desert One, and provide cyber forces with interoperable, capable cyber weapons and systems in a streamlined, efficient fashion.

Doctrine

The move to cyber-centric operations requires significant development in the area of cyberspace doctrine. While the Air Force and Army are moving in the same general direction, the Navy continues to use the archaic CNO doctrine. Besides the services, there is no shortage of other organizations providing doctrine: the Office of Secretary of Defense (OSD), the Joint Staff (JS), combatant commands, DHS through the US Computer Emergency Readiness Team, and even the White House. In spite of the large number of cyberspace theorists, no clearinghouse exists to de-conflict, adjudicate, or synchronize the ideas emanating from the various organizations. When cyberspace operators from different services operate in the same

cyber quadrants with conflicting techniques, tactics, and procedures (TTPs), disaster can result. Cyber response actions, such as those for responding to catastrophic cyber network outages or cyber attacks, should be standardized and available for training and educating cyber forces. Additionally, cyber operations require different approaches due to the irrelevance of distance and speed in cyberspace, forcing the development of new doctrine.[26] Until the DoD designates a single authority for cyber doctrine, each organization will continue to develop and use its own ideas, regardless of their compatibility with other DoD agencies.

The DoD, by capitalizing on the USSOCOM example, could designate a single, authoritative command for the development and adjudication of cyberspace doctrine, strategy, and TTPs. As the single entity in DoD responsible for doctrine, cyber command can leverage the strengths of the services, OSD, JS, and other agencies to develop ideas, and serve as the single approval authority for codifying doctrine as official. Since the cyber environment creates the need to organize, train, and equip in non-traditional ways, cyber command – the organization with the preponderance of cyberspace experts – is the perfect organization to develop the strategy to address this new frontier[27]. In addition to managing DoD cyberspace doctrine, cyber command would also de-conflict service-centric doctrine to ensure force interoperability and seamless integration of components for JFC operational missions. By establishing standardized cyber response actions, independent cyber forces from different services or agencies can safely operate in cyberspace when disaster, or enemies, strike our cyber infrastructure.

Conclusion

The potential for operations in cyberspace is only matched by the vulnerabilities it creates to our national defense. US critical infrastructures depend on freedom of action in cyberspace to provide essential services to our citizenry. Within the DoD, service-centric cyber force

development, an ineffective cyber organizational structure, weak C2 of cyber forces, and limited oversight of cyber technology and personnel development hinders our ability to defend US interests in cyberspace. To ensure our continued superiority in the cyber domain, the DoD should adopt the USSOCOM structure for organizing, equipping, and leading cyber forces. The USSOCOM model, with its distinctive blend of combatant command authority and service-like responsibilities, provides significant advantages for cyberspace organizational structure, cyber personnel management, cyber weapons and systems development, and cyberspace doctrine. While some might argue for a new combatant command for cyberspace, establishing a sub-unified command for cyberspace under the purview of USSTRATCOM is also a viable option. Ultimately, as long as the DoD designates a single organization responsible for cyberspace based on the USSOCOM template, the US will maintain cyber superiority and protect its national interests in cyberspace.

Endnotes

[1] White House, *The National Strategy to Secure Cyberspace* (Washington, DC: White House, February 2003), 1, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf (accessed January 19, 2009).

[2] Joint Chiefs of Staff, Command, Control, Communications, and Computer Systems Directorate, *Joint Net-Centric Operations Campaign Plan* (Washington, DC: Joint Chiefs of Staff, October 2006), 62, http://www.jcs.mil/j6/c4campaignplan/JNO_Campaign_Plan.pdf (accessed January 19, 2009).

[3] US Department of Defense, "Memorandum for Secretaries of the Military Departments: The Definition of Cyberspace", by Deputy Defense Secretary Gordon England (Washington, DC: Department of Defense, May 2008), 1, http://www.afei.org/documents/NewCyberspaceDefinition.pdf (accessed January 19, 2009).

[4] Headquarters US Air Force, *The Air Force Roadmap for the Development of Cyberspace Professionals: 2008-2018* (Washington, DC: Headquarters US Air Force, April 2008), 2-4.

[5] Ibid., 4-7.

[6] Ibid., 8-9.

[7] Ibid., 9-14.

[8] Lieutenant Colonel Brian D. Glando, "How is the Army Developing Cyber Warriors?" Information Paper, US Department of the Army, 2008.

[9] US Department of the Army, "Cyberspace Career Field: Chief of Staff of the Army Briefing," Pre-Decisional Briefing, US Department of the Army, 2008.

[10] Ibid.

[11] US Marine Corps Cryptologic Support Battalion, "Computer Network Operations: Company L, MCSB," Informational Briefing and Paper, US Marine Corps, 2009.

[12] US Strategic Command, "US Strategic Command Fact Sheets," US Strategic Command Home Page, January 2009. http://www.stratcom.mil/default.asp?page=factsheets (accessed January 20, 2009).

[13] Ibid.

[14] US Special Operations Command, *US Special Operations Command History: 1987-2007* (MacDill Air Force Base, FL: US Special Operations Command, February 2007), 5-7,

http://www.socom.mil/Docs/Command_History_26Feb07webversion.pdf (accessed January 9, 2009).

[15] Admiral Eric T. Olson, "US Special Operations Command" (Command and Staff College lecture, Marine Corps University, Quantico, VA, January 22, 2009).

[16] D. Robert Worley, *Shaping US Military Forces* (Westport, CT: Praeger Security International, 2006), 241.

[17] Admiral Olson lecture.

[18] Robert G. Spulak, Jr., "A Theory of Special Operations: The Origin, Qualities, and Use of SOF" (Joint Special Operations University Report 07-7, October 2007), 15.

[19] Ibid., 19.

[20] David Tucker and Christopher J. Lamb, *United States Special Operations Forces* (New York: Columbia University Press, 2007), xv-xvii.

[21] Ibid., 39, 45, 47, 185-186.

[22] US Strategic Command, *Joint Concept of Operations for Global Information Grid NetOps, Version 3* (Offutt Air Force Base, NE: US Strategic Command, August 2006).

[23] Brigadier General Jennifer L. Napper, Email message to author, October 7, 2008.

[24] Ibid.

[25] Lieutenant Colonel Sebastian M. Convertino, Lou Anne DeMattei, and Lieutenant Colonel Tammy M. Knierim, *Flying and Fighting in Cyberspace*, Air War College Maxwell Paper No. 40 (Maxwell Air Force Base, AL: Air University Press, 2007), 69.

[26] Ibid., 71.

[27] Ibid., 71.

Bibliography

Convertino, Lieutenant Colonel Sebastian M., Lou Anne DeMattei, and Lieutenant Colonel Tammy M. Knierim. *Flying and Fighting in Cyberspace*. Air War College Maxwell Paper No. 40. Maxwell Air Force Base, AL: Air University Press, 2007.

Glando, Lieutenant Colonel Brian D. "How is the Army Developing Cyber Warriors?" Information Paper, US Department of the Army, 2008.

Hall, Colonel Bill. "Force Development for Cyber Transformation." Information Briefing, Headquarters US Air Force, 2008.

Headquarters US Air Force. *The Air Force Roadmap for the Development of Cyberspace Professionals: 2008-2018.* Washington, DC: Headquarters US Air Force, April 2008.

Joint Chiefs of Staff. Command, Control, Communications, and Computer Systems Directorate. *Joint Net-Centric Operations Campaign Plan.* Washington, DC: Joint Chiefs of Staff, October 2006. http://www.jcs.mil/j6/c4campaignplan/JNO_Campaign_Plan.pdf (accessed January 19, 2009).

Napper, Brigadier General Jennifer L. Email message to author, October 7, 2008.

Olson, Admiral Eric T. "US Special Operations Command." Command and Staff College lecture, Marine Corps University, Quantico, VA, January 22, 2009.

Spulak, Robert G. Jr. "A Theory of Special Operations: The Origin, Qualities, and Use of SOF." Joint Special Operations University Report 07-7, October 2007.

Tucker, David, and Christopher J. Lamb. *United States Special Operations Forces*. New York: Columbia University Press, 2007.

US Department of the Army. "Cyberspace Career Field: Chief of Staff of the Army Briefing." Pre-Decisional Briefing, US Department of the Army, 2008.

US Department of Defense. "Memorandum for Secretaries of the Military Departments: The Definition of Cyberspace", by Deputy Defense Secretary Gordon England. Washington, DC: Department of Defense, May 2008.
http://www.afei.org/documents/NewCyberspaceDefinition.pdf (accessed January 19, 2009).

US Marine Corps Cryptologic Support Battalion. "Computer Network Operations: Company L, MCSB." Informational Briefing and Paper, US Marine Corps, 2009.

US Special Operations Command. *US Special Operations Command History: 1987-2007.* MacDill Air Force Base, FL: US Special Operations Command, February 2007. http://www.socom.mil/Docs/Command_History_26Feb07webversion.pdf (accessed January 9, 2009).

US Strategic Command. *Joint Concept of Operations for Global Information Grid NetOps, Version 3.* Offutt Air Force Base, NE: US Strategic Command, August 2006.

US Strategic Command. "US Strategic Command Fact Sheets." US Strategic Command Home Page, January 2009. http://www.stratcom.mil/default.asp?page=factsheets (accessed January 20, 2009).

White House. *The National Strategy to Secure Cyberspace.* Washington, DC: White House, February 2003. http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf (accessed January 19, 2009).

Worley, D. Robert. *Shaping US Military Forces.* Westport, CT: Praeger Security International, 2006.