REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04-05-2011	FINAL	

4. TITLE AND SUBTITLE

Organize and Optimize: CYBERCOM's Need to be a Unified Command

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Tamara M. Keene, Major, USAF

Paper Advisor (if Any): Reagan Schaupp, Lt Col, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

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

Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The recent establishment of the United States Cyber Command as a sub-unified command under United States Strategic Command is not optimized. Cyber Command should be a full functional unified command. The analysis will discuss why a unified command structure is preferred over a sub-unified command structure. Concentration on command and control, external relationships, and joint force presentation provide the reader focus areas. Joint Publication 1 helps explain the intricacies of joint force structures. This is then applied to the domain of cyberspace. Individual Service application is briefly discussed and how it relates to the bigger picture. Operational factors of time and space are discussed throughout. Recommend clarifying terminology throughout the Department of Defense in order to ensure a smooth transition to a functional unified command.

15. SUBJECT TERMS

CYBERCOM, JP1, cyberspace, unified command, sub-unified command

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		23	19b. TELEPHONE NUMBER *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

ORGANIZE AND OPTIMIZE: CYBERCOM'S NEED TO BE A UNIFIED COMMAND

by

Tamara M. Keene

Major, United States Air Force

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____//signed//_____

4 May 2011

Contents

Abstract

The recent establishment of the United States Cyber Command as a sub-unified command under United States Strategic Command is not optimized. Cyber Command should be a full functional unified command. The analysis will discuss why a unified command structure is preferred over a sub-unified command structure. Concentration on command and control, external relationships, and joint force presentation provide the reader focus areas. Joint Publication 1 helps explain the intricacies of joint force structures. This is then applied to the domain of cyberspace. Individual Service application is briefly discussed and how it relates to the bigger picture. Operational factors of time and space are discussed throughout. Recommend clarifying terminology throughout the Department of Defense in order to ensure a smooth transition to a functional unified command.

INTRODUCTION

In today's technologically-laden world, it is hard to imagine what life was like before the proliferation of cyberspace. Basic communications have evolved from handwritten letters to typed email, reducing the communication timeline from weeks to seconds-regardless of distance. Our lives are bombarded with conveniences offered through the use of cyberspace – and we have reached a point where it would be very hard to go back.

In the Department of Defense, a similar transformation occurred. The Honorable William J. Lynn, III summarized its role in the Department: "in less than a generation, information technology in the military has evolved from an administrative tool for enhancing office productivity into a national strategic asset in its own right."[1] Today, our military depends on cyberspace to support its use of military forces throughout the world. However, this dependence brings risks. Risks like network outages due to lack of power or risks like denial of service or data corruption due to a virus. In order to minimize these and other possible risks, U.S. Secretary of Defense Robert Gates established the United States Cyber Command (CYBERCOM) as a sub-unified command under the United States Strategic Command (STRATCOM).

CYBERCOM should be realigned as a functional unified command to optimize command and control, external agency coordination, and joint force presentation to combatant commanders.

DISCUSSION / ANALYSIS

What is cyberspace?

So what is cyberspace exactly? In order to facilitate discussion, it is important to have a common understanding of the term. The very definition of cyberspace varies widely across doctrine. This lack of consensus on what cyberspace is contributes to the confusion regarding how to operate in it. The 2003 National Strategy to Secure Cyberspace offers a vague definition of "…the control system of our country…hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructures work…essential to our economy and national security."[2] The 2011 National Military Strategy (NMS) refers to cyberspace over five times as often as the previous version, and yet a solid definition of what cyberspace actually is cannot be found.[3] Joint Publication 1-02 defines 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."[4] Accordingly, everything from home computers to bank networks to power plants is considered part of cyberspace. Thus, the need to maintain freedom of movement within cyberspace is vital not only to the military, but to our national security as well.

Cyberspace is global. The NMS refers to cyberspace as a "globally connected domain."[5] Unlike land, air, and sea, it does not have traditional borders that are definable by coordinates or distances. Further complicating the domain is that it is shared by military and civilian populations alike.

Much like land, air, sea and space, cyberspace is an operational environment. Rear Admiral William Leigher, deputy commander of U.S. Fleet Cyber Command, U.S. Tenth Fleet, notes in his article titled "Learning to Operate in Cyberspace" that some may not view

cyberspace as a domain since, unlike the other four domains, it is manmade.[6] However, he then argues that "cyberspace is physically just as real as the other four domains."[7] This inability to "see" or physically define the limits of cyberspace can cause confusion when trying to discuss cyberspace as an operational domain. The traditional thinking that applies to land, air and sea may not apply directly to cyberspace. The operational factors of time and space are tougher to conceptualize in this domain.

The operational factor of time is theoretically much faster than in the other domains. Not only is the domain itself inherently faster, but the timely movement of forces or objects from physical point A to physical point B within the traditional domains is perhaps unnecessary in cyberspace. Space is much harder to discuss in this domain – it is often undefined or perhaps even irrelevant. The globally shared nature of cyberspace causes the factor of space to be tricky when trying to understand its effect on military objectives.

But how does cyberspace help combatant commanders achieve their objectives? The NMS states that "cyberspace capabilities enable Combatant Commanders to operate effectively across all domains"[8] and "space and cyberspace enable effective global warfighting in the air, land, and maritime domains, and have emerged as war-fighting domains in their own right."[9] Therefore, the NMS not only acknowledges the necessity for the military to have freedom in cyberspace but also notes that it may be a venue for military conflict.

The Department of Defense (DOD) achieves their objectives within the cyberspace domain through cyberspace operations. Joint Publication 1-02 defines cyberspace operations as "the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and

activities to operate and defend the Global Information Grid."[10] Cyber Command is responsible for cyberspace operations within the DOD.

Sub-unified Versus Unified Commands

The difference between a sub-unified command and a unified command is subtle. Sub-unified commands have been around almost as long as unified commands – as early as 1948, the Key West Agreement gave unified commanders the authority to create sub-unified commands just two years after the first unified command plan.[11] Joint Publication 1-0 defines a unified command as "a command with broad continuing missions under a single commander"[12] whereas the same publication defines a sub-unified command as one responsible to "conduct operations on a continuing basis in accordance with the criteria set forth for unified commands."[13] In other words, a combatant commander can establish a sub-unified command in order to divide his responsibilities into more manageable pieces. Although this delegated responsibility appears to be an attempt to better the command and control within a command, in the case of CYBERCOM it may be harmful because it obscures the command and control, it confuses external coordination, and it allows for an unsynchronized force presentation to the Combatant Commanders. JP 1 further delineates the requirements for a unified command.

JP 1 details two criteria for unified command establishment "when either or both of the following criteria apply generally to a situation, a unified command normally is required to ensure unity of effort."[14] The first criteria, "a broad continuing mission exists requiring execution by significant forces of two or more Military Departments and necessitating a single strategic direction"[15] describes the cyberspace mission. Cyberspace requires forces of all of the Military Departments, although the term "significant" is perhaps debatable.

The second criteria lists three qualifiers of which only one or more must apply. For cyberspace, the second sub-criteria is met as it is "a large geographic or functional area requiring single responsibility for effective coordination of the operations."[16] Due to the unique characteristics of the domain (global, shared), one organization needs to be in charge of cyberspace operations. Thus, by JP 1 definition, cyberspace should be a unified command to better unity of effort.

Command and Control

CYBERCOM's command and control would be best suited through a functional unified command structure. JP 1 defines four principles for effective command and control within a joint force: simplicity, span of control, unit integrity, and interoperability.[17] These four principles provide a framework to discuss how command and control will benefit from a unified command structure.

The first principle is simplicity. JP 1 defines simplicity as "an unambiguous chain of command, well-defined command relationships, and clear delineation of responsibilities and authorities."[18] The command and control structure of Cyber Command, as a sub-unified command, lacks in this principle. The Services each present forces to STRATCOM which places them under operational control (OPCON) of CYBERCOM. In a domain where the factor of time and space are so fast and virtually compressed, a convoluted chain of command will present unnecessary delays. Making CYBERCOM a combatant command would streamline the chain of command and therefore maximize the flexibility of cyberspace operations.

JP 1 stresses the importance of "the JFC's ability to C2 the actions required"[19] in the second principle, span of control. In other words, the JFC needs to be able to C2 everything

assigned under him/her – if not, the span of control is perhaps too wide and needs to be lessened. The placement of CYBERCOM under STRATCOM is problematic in this area. STRATCOM is currently responsible "planning, synchronizing, advocating, and employing capabilities to meet the nation's strategic deterrence, space operations, cyberspace operations, information operations, global strike, missile defense, intelligence, surveillance, reconnaissance, and combating weapons of mass destruction objectives."[20] In fact, the 2011 Unified Command Plan added to "U.S. Strategic Command's responsibility for combating weapons of mass destruction and developing Global Missile Defense Concept of Operations."[21] A broad and diverse mission set. USSTRATCOM Commander, General C. Robert Kehler, confirms his organization's focus as "first and foremost, we must guarantee a safe, secure, effective, and ready nuclear deterrent force."[22] While acknowledging the seriousness of the mission to deter nuclear attack, placing CYBERCOM within STRATCOM is causing the organization's mission to be too broad, violating the principle of span of control. The nuclear mission will remain number one – but will that be to the detriment of cyberspace?

Some may argue that CYBERCOM is a sub-unified command under STRATCOM for the very reason of span of control. It is the unified commander's prerogative to create a sub-unified command in order to delegate and focus one particular area within his mission set. Regardless of this subdivision of labor, the overall unified commander still retains command, and thus interest and time, over the sub-unified command.

The third principle, unit integrity, emphasizes that "component forces should remain organized as designed and in the manner accustomed through training to maximize

effectiveness."[23] This principle does not impact the unified/sub-unified decision as the component forces will have unit integrity regardless.

Interoperability is the fourth principle of effective C2 of joint forces. JP 1 emphasizes that "C2 capabilities within joint force headquarters, component commands, and other supporting commands must be interoperable to facilitate control of forces."[24] CYBERCOM, as a sub-unified command, hinders interoperability efforts among the services. In 2009, Vice Admiral Nancy Brown, Director of Command and Control Directorate of the Joint Staff, commented on the cross-Service interoperability challenge: "we have multiple infrastructures that have evolved to solve specific problems in a service specific way, and which may be duplicated by another service or agency to solve the same problem in a different way."[25] Her concern is that "the combatant commander should be thinking about how to use the network to plan, attack, defend, and so forth, not thinking about how to kludge together disparate systems."[26] The operational factors of time and space, when dealing in cyberspace, amplify the need for this interoperability. As a unified command, like SOCOM, there would be a more conscious effort to ensure interoperability between Services.

The Department of Defense has dealt with the command and control issue before. The early 1980s were cause for concern within the Department of Defense as lives were lost due to apparent command and control issues within the special operations forces.[27] This concern led to congressional inquiries that resulted in the conclusion that "the U.S. needed a clearer organizational focus and chain of command for special operations to deal with low-intensity conflicts."[28] The Joint Special Operations Agency was established in 1984 to try to address some of the problems but two years later the JSOA's director "frankly described the

agency's coordinating efforts as a 'failure'."[29] Thus, Special Operations Command was born as a full unified command and remains one today. CYBERCOM should be a unified command, like SOCOM, in order to optimize command and control.

External Relationships

Clear external organizational relationships are needed for CYBERCOM. Similar to the concept of simplicity for internal command and control, external relationships need to be clear and concise. As a sub-unified command, exterior relationships are brokered through STRATCOM or at least through a liaison, adding a layer of delay and perhaps confusion.

CYBERCOM is engaged in a "strategic partnership with the Department of Homeland Security."[30] This relationship is one example of an external agency or department that Cyber Command works closely with. In fact, external relationships are one of the five strategic initiatives laid out by General Alexander: "partner closely with other U.S. government departments and agencies and the private sector to enable a whole-of-government strategy and an integrated national approach to cyber security."[31] This interagency coordination will work better if Cyber Command is a unified command because it will eliminate the need to go through USSTRATCOM whenever a relationship needs to be established. The impact of time and space on the domain stresses the need for the quick establishment of direct lines of communication.

Of course, critics could say that this external agency coordination is the situation that "DIRLAUTH" was created for – "Direct Liaison Authority." DIRLAUTH, according to JP 1, "is that authority granted by a CDR (any level) to a subordinate to directly consult or coordinate an action with a command or agency within or outside of the granting command."[32] That definition sounds like it would work. In fact, in However, JP 1 continues

to emphasize that this relationship is usually used for planning as opposed to operations and "always carries with it the requirement of keeping the CDR granting DIRLAUTH informed."[33] Keeping USSTRATCOM in the loop is too time-consuming for this domain.

Joint Force Presentation

The four Services recently testified to Congress's House Armed Services Committee regarding their respective Services' methods to meet cyber challenges. The testimony shows that each Service approaches the cyberspace realm in a slightly different manner. These differences can hinder getting cyber capability to the Combatant Commander. As a result, CYBERCOM should be a combatant command with a more joint presentation of forces.

Today, Cyber Command is still developing how to present forces to Combatant Commanders. General Alexander testified that "Service cyber components were formally assigned to USSTRATCOM."[34] He also noted that "we embedded liaison officers at Combatant Commands and set conditions to expand their presence to larger Cyber Support Elements."[35] However, the Services seem to be off-script in how to present forces to the combatant commander.

The Navy presents forces in a way similar to "a typical Navy Task Force Organization. This structure assigns regional responsibilities to subordinate task groups."[36] That unit is Fleet Cyber Command and according to testimony they "directs cyberspace operations in defense and support of our forces to deter and defeat aggression and ensure freedom of action."[37]

The Navy stresses the relationship between the Services as one of sharing in order to create a better defense. The commander of United States Fleet Cyber Command, Admiral Bernard McCullough III, testified that "as a supporting command to U.S. Cyber Command,

we are using the commonalities between service components to build a network defense-in-depth architecture, allowing our diverse capabilities to create robust and adaptable global cyber defense. If one service discovers, analyzes and defeats a threat, that information can be rapidly disseminated to the other Services to minimize any intrusion effort and create a unified response."[38] On one hand, the concept of the Services sharing information in this manner is commendable but on the other it sounds like possible duplication of effort. While the Navy stresses sharing amongst the Services, the other Services are a little less forthcoming.

The Air Force acknowledges there may be duplication of effort amongst the Services. The AFCYBER commander, Major General Richard Webber noted "as we share our situational awareness planning efforts with USCYBERCOM, their overall understanding of each of the services' efforts will prevent wasteful duplication of effort."[39] Establishing CYBERCOM as a full unified command will give CYBERCOM legitimacy in creating joint operations by erasing the Service duplication.

The Air Force sees cyberspace as something that is service-specific despite the global, shared nature discussed above. Major General Webber explained that "establishing 24 AF created one commander to oversee Cyber operations for the AF and gave that commander authority no previous entity had to enact the changes necessary to operationalize AF Cyber."[40] Note the use of the term "AF Cyber."[41] In other words, the AF still views cyberspace as a domain to be parsed into several little domains with individual owners. The AF is not the only service to protect their piece of the network as their own.

Like the AF, the Army sees the network (a part of cyberspace) as something they can divide up. The director of the Army Cyberspace Task Force, Maj Gen Steven W. Smith,

stated that "the mission for ARFORCYBER is to direct the operation and defense of all Army networks, and, on order, conduct full-spectrum operations in support of our combatant commanders and coalition partners."[42] He specifically points out their mission regarding the Army networks. In this domain, we need to start thinking at an enterprise (Department of Defense) level as opposed to specific Service. This will provide a better force presentation to the combatant commanders because it will standardize the capability across the joint force. A combatant commander will not be faced with a force made up of people who know how to operate the AF network or the Army network etc, he will be presented with a force that can maneuver within cyberspace regardless of which Service may happen to own a piece of hardware.

The Marine Corps view of cyberspace is similar to the other services in that they focus on their own domain. Congressional testimony regarding cyberspace noted that "MARFORCYBER will plan, coordinate, integrate, synchronize and direct *defensive* cyberspace operations to *preserve* the Marine Corps ability to use and function within the Marine Corps Enterprise Network (MCEN)." (emphasis in original)[43] Additionally, "MARFORCYBER provides support to USCYBERCOM as the Marine Corps' Service Component."[44]

The above discussion regarding the Services highlights the "my sandbox" mentality that still permeates the Services thinking regarding cyberspace. The establishment of a combatant command would minimize this by streamlining these efforts under a common command. It also highlights that each Service is defending their own network (ie, domain) and is sharing their network feeds (common operating picture per say) with the other Services (and with Cyber Command). Lieutenant Colonel David Hollis, a joint plans officer

at STRATCOM, believes that "because of the unique nature of the domain, no one Service is responsible for operations to protect national cyberspace (unlike the other domains); a full COCOM would be better resourced and have greater authority and responsibility to compensate for the lack of a specific Service lead."[45] Cyber Command could operate the enterprise as opposed to the Services operating their own domains within cyberspace.

Some services take the "my domain" concept further. The Air Force is currently presenting cyber forces to the Air Operations Center through the concept of COLE, or a Cyber Operations Liaison Element, based off the Special Operations construct of SOLE.[46] Congressional testimony said that this liaison arrangement is to "facilitate the requisite exchange of expertise between mission planners and Cyber planners."[47] While this may not be a bad concept overall, it should be CYBERCOM that gives that capability to an AOC. Further complicating this concept are the abovementioned liaison officers at combatant commands. Does the COLE work through the liaison officer at the higher level combatant command or directly back to 24th AF?

It is important to see how the Services view cyber so to understand how they are allocating their personnel. General Alexander noted this tension that the Services are under by stating "there are too few trained Service personnel out there in the first place, and also the Services need to hold on to as many of them as they can."[48] This tension has caused the DOD to "not have the capacity to do everything we need to accomplish"[49] and that "a crisis would quickly stress our cyber forces."[50] He further explains that there is a "need for collaborative force development (including joint standards, recruitment, training, deployment, sustainment, and retention)."[51] A unified command would foster this collaborative environment.

There are several good arguments for why Cyber Command needs to be a unified command. Effective command and control, interagency relationships, and joint force presentation are just three of them. There are, however, a few arguments for why Cyber Command should remain a sub-unified command. There are historical and financial arguments against making it a unified command.

Counterargument

Many believe that CYBERCOM should remain a sub-unified command. There are two main reasons that could support the sub-unified command argument – historical and financial.

Historically, some liken cyber to space. Some involved in making the CYBERCOM decision were afraid to "make the Space Command mistake again."[52] In his book Cyber War, author Richard Clarke claims that "they did not want to create a Unified Command for what might be a passing fad, as war fighting in space had been."[53] This argument, however, does not hold much weight as history shows a dynamic and changing Unified Command Plan. The fact that USSPACECOM did not "last" as a unified command is simply not a reflection on its mission – it is a product of the continued refinement of the overall plan. USSPACECOM, established in 1985[54], lived a short life as a unified command – being disestablished in 2002.[55]

While space is no longer a unified command, it was the right move at that time in order to ensure effective command and control of the joint force. The establishment of the unified command enabled processes, procedures, and training to be created that benefited the joint force – more so than would have happened if it had not been a unified command.

Cyberspace deserves that same attention at the beginning – a chance to establish a set of joint processes and procedures that can ensure our freedom of action throughout the domain.

In today's fiscally-constrained environment, it is easy to argue against the establishment of a full unified command due to money. This is not a new argument of course. In August 2010, Defense Secretary Gates recommended the disestablishment of Joint Forces Command as part of a multi-step proposal aimed to "reduce overhead, duplication, and excess in the Department of Defense, and, over time, instill a culture of savings and restraint in America's defense institutions."[56] In the same proposal, he also "directed a freeze in the number…of COCOM billets at the fiscal 2010 levels."[57] These recommendations complicate any discussion of creating a new unified command. It is a hard sell to create a new unified command when another is planned to be closed within the year for essentially financial reasons. However, it is not a decision to be made by the bottom line alone. Defense Secretary Gates announced $1.2 billion in reductions in information technology over the five year defense plan.[58] Given such a restricted budgetary environment, it seems counter-intuitive to recommend the establishment of a new unified command. However, through the optimization of command and control and joint presentation of forces, there may be savings in creating a unified command.

CONCLUSIONS and RECOMMENDATIONS

A recent *Air and Space Power Journal* article titled "War Fighting in Cyberspace: Evolving Force Presentation and Command and Control"[59] recognized that today's force structure needs improvement. The author laid out a three-step plan to move from the current posture to reach a unified command.[60] Regardless of how we get there, the Department of Defense needs to have a unified command in charge of the cyberspace domain. The unified

command structure enables an overarching reality: that the "Armed Forces of the United States are most effective when employed as a joint force."[61] The reasons described above outline why a sub-unified command will not suffice in the long run. For smooth joint operations, command and control must adhere to the four principles of command and control and a unified command fosters the optimization of these principles. For synchronized cyberspace operations, clear external relationships are needed and a unified command structure will help external agencies in their coordination with CYBERCOM. For a consistent and useful capability to be delivered to the combatant commanders, a synchronized joint force presentation needs to be adopted – a dream that will flourish under a unified command structure.

The journey to create a unified command will be smoother if all of the Services could agree on what it means to operate in cyberspace. Also, we should make a clear distinction between cyberspace operations and the building and maintenance of physical networks. Similar to the relationship between a pilot and the maintainer, or the pilot and the contractor who built the plane, a cyberspace operator should not be the same person that maintains or builds the network. Unfortunately, this relationship varies amongst the Services and hinders joint efforts until it is resolved. Therefore, to ensure a successful transition to a full unified command, each Service should delineate between the operators and the maintainers/builders of cyberspace. This clarity will not only help propel joint discussions but will save additional manpower as the operators can be centrally located while only the maintainers/builders have to be in local proximity to the network itself.

FINAL REMARKS

Chairman Ike Skelton summarized it pretty well in his opening statement. He said "of one thing I am confident, cyberspace will be a big part of the future of warfare. That means we can't afford to get this wrong. The establishment of CyberCom is a critical milestone for this nation's defense."[62] He is absolutely right – we must organize and operate for success within cyberspace from the beginning. And the first step is to create a combatant command with clear command and control, external relationships, and joint force presentation to the supported combatant commanders.

NOTES

1. William J. Lynn III,"Defending a New Domain," *Foreign Affairs* 89 iss.3 (Sep/Oct 2010), http://www.proquest.com/ (accessed 10 April 2011).
2. U.S. President, *The National Strategy to Secure Cyberspace*. (Washington, DC: White House, 2003). http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (accessed 10 April 2011), 1.
3. Chairman, U.S. Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2011:Redefining America's Leadership.* (Washington, DC: CJCS, 2011). http://www.jcs.mil/content/files/2011-02/020811084800_2011_NMS_-_08_FEB_2011.pdf (accessed 10 April 2011).
4. Chairman, U.S. Joint Chiefs of Staff, *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*. Washington, DC: CJCS, 8 November 2010 (amended through 31 January 2011. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed 13 April 2011), 93.
5. Chairman, U.S. Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2011:Redefining America's Leadership* (Washington, DC: CJCS, 2011), http://www.jcs.mil/content/files/2011-02/020811084800_2011_NMS_-_08_FEB_2011.pdf (accessed 10 April 2011), 3.
6. William Leigber, "Learning to Operate in Cyberspace," Proceedings (February 2011), Vol 137, Iss 2: 32-38. http://www.proquest.com/ (accessed 27 March 2010).
7. Ibid.
8. Chairman, U.S. Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2011:Redefining America's Leadership* (Washington, DC: CJCS, 2011), http://www.jcs.mil/content/files/2011-02/020811084800_2011_NMS_-_08_FEB_2011.pdf (accessed 10 April 2011), 10.
9. Ibid, 9.
10. Chairman, U.S. Joint Chiefs of Staff. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*. Washington, DC: CJCS, 8 November 2010 amended through 31 January 2011. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed 13 April 2011), 93.
11. Joint History Office, Office of the Chairman of the Joint Chiefs of Staff, *The History of the Unified Command Plan 1946-1999* (Washington, DC: Government Printing Office, 2003), 15.
12. Chairman, U.S. Joint Chiefs of Staff. *Joint Publication 1: Doctrine for the Armed Forces of the United States*. Washington, DC: CJCS, 2 May 2007 amended through 20 March 2009. http://www.dtic.mil/doctrine/new_pubs/jp1.pdf (accessed 13 April 2011), V-5.
13. Ibid, V-9.
14. Ibid, V-5.
15. Ibid, V-5.
16. Ibid, V-5.
17. Ibid, IV-19.
18. Ibid, IV-19.
19. Ibid, IV-19.

20. C. Robert Kehler, "Testimony," House, *Statement of General C. Robert Kehler Commander United States Strategic Command before the Senate Committee on Armed Services,* 112th Cong., 1st sess., 2011, http://armed-services.senate.gov/statemnt/2011/03%20March/Kehler%2003-29-11.pdf (accessed 3 May 2011), 1.
21. U.S. Defense Department. "DOD Releases Unified Command Plan 2011," News Release, 8 April 2011, http://www.defense.gov/releases/release.aspx?releaseid=14398 (accessed 4 May 2011).
22. C. Robert Kehler, "Testimony," House, *Statement of General C. Robert Kehler Commander United States Strategic Command before the Senate Committee on Armed Services,* 112th Cong., 1st sess., 2011, http://armed-services.senate.gov/statemnt/2011/03%20March/Kehler%2003-29-11.pdf (accessed 3 May 2011), 3.
23. Chairman, U.S. Joint Chiefs of Staff. *Joint Publication 1: Doctrine for the Armed Forces of the United States*. Washington, DC: CJCS, 2 May 2007 amended through 20 March 2009. http://www.dtic.mil/doctrine/new_pubs/jp1.pdf (accessed 13 April 2011), IV-19.
24. Ibid, IV-19.
25. Nancy E. Brown, "Difficulties Encountered as We Evolve the Cyber Landscape for the Military," *High Frontier: The Journal for Space & Missile Professions* 5, no. 3 (May 2009), http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf (accessed 3 May 2011), 7.
26 Ibid, 7.
27. United States Special Operations Command, "US SOCOM History," http://www.socom.mil/SOCOMHome/Pages/History.aspx (accessed 9 April 2011).
28. Ibid.
29. Joint History Office, Office of the Chairman of the Joint Chiefs of Staff, *The History of the Unified Command Plan 1946-1999* (Washington, DC: Government Printing Office, 2003), 83.
30. Keith Alexander, "Testimony," House, *2012 Budget Request from U.S. Cyber Command: Hearing before the House Committee of Armed Services Subcommittee on Emerging Threats and Capabilities,* 112th Cong., 1st sess., 2011, http://armedservices.house.gov/index.cfm/files/serve?File_id=50aeaaff-808b-4f43-a8d0-ad86ec9357f6 (accessed 18 April 2011), 13.
31. Ibid, 10.
32. Chairman, Joint Chiefs of Staff. Joint Publication 1: Doctrine for the Armed Forces of the United States. Washington, DC: CJCS, 2 May 2007 amended through 20 March 2009. http://www.dtic.mil/doctrine/new_pubs/jp1.pdf (accessed 13 April 2011), IV-13.
33. Ibid, IV-13.
34. Keith Alexander, "Testimony," House, *2012 Budget Request from U.S. Cyber Command: Hearing before the House Committee of Armed Services Subcommittee on Emerging Threats and Capabilities,* 112th Cong., 1st sess., 2011, http://armedservices.house.gov/index.cfm/files/serve?File_id=50aeaaff-808b-4f43-a8d0-ad86ec9357f6 (accessed 18 April 2011), 3.
35. Ibid, 3.

36. Bernard McCullough, "Testimony," House, *Terrorism, Unconventional Threats, and Capabilities Subcommittee: Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations*. 111th Cong., 2nd sess., 2010, http://democrats.armedservices.house.gov/index.cfm/files/serve?File_id=46ab9cfd-c2a2-4529-a8bf-49413b1df8bf (accessed 7 April 2011), 2.
37. Ibid,1.
38. Ibid, 4.
39. Richard Webber, "Testimony," House, *Terrorism, Unconventional Threats, and Capabilities Subcommittee: Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations*. 111th Cong., 2nd sess., 2010, http://democrats.armedservices.house.gov/index.cfm/files/serve?File_id=8b28f10f-e164-481f-93cc-0c0734195fb1 (accessed 7 April 2011), 9.
40. Ibid, 5.
41. Ibid, 5.
42. C. Todd Lopez, "Cyber Command to Unite Network Defense Efforts," *army.mil*, 2 June 2010, http://www.army.mil/-news/2010/06/02/40195-cyber-command-to-unite-network-defense-efforts/ (accessed 4 May 2011).
43. George Flynn, "Testimony," House, *Terrorism, Unconventional Threats, and Capabilities Subcommittee: Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations*. 111th Cong., 2nd sess., 2010, http://democrats.armedservices.house.gov/index.cfm/files/serve?File_id=d95a1fa0-48d3-4d57-93d3-ccaf4efbd848 (accessed 7 April 2011).
44. Ibid
45. David Hollis, "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command," *ndu.edu*, **http://www.ndu.edu/press/USCYBERCOM.html** (accessed 23 February 2011).
46. Richard Webber, "Testimony," House, *Terrorism, Unconventional Threats, and Capabilities Subcommittee: Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations*. 111th Cong., 2nd sess., 2010, http://democrats.armedservices.house.gov/index.cfm/files/serve?File_id=8b28f10f-e164-481f-93cc-0c0734195fb1 (accessed 7 April 2011), 7.
47. Ibid, 7.
48. Keith Alexander, "Testimony," House, *2012 Budget Request from U.S. Cyber Command: Hearing before the House Committee of Armed Services Subcommittee on Emerging Threats and Capabilities*, 112th Cong., 1st sess., 2011, http://armedservices.house.gov/index.cfm/files/serve?File_id=50aeaaff-808b-4f43-a8d0-ad86ec9357f6 (accessed 18 April 2011), 16.
49. Ibid, 16.
50. Ibid, 16.
51. Ibid, 16.
52. Richard A. Clarke and Robert K. Knake, *Cyber War* (New York, NY: HarperCollins Publishers 2010), 36.
53. Ibid, 37

54. Joint History Office, Office of the Chairman of the Joint Chiefs of Staff, *The History of the Unified Command Plan 1946-1999* (Washington, DC: Government Printing Office, 2003), 82.
55. United States Strategic Command, http://www.stratcom.mil/history/ (accessed 2 May 2011).
56. U.S. Defense Department. "Sec. Gates Announces Efficiencies Initiatives," *News Release*, 9 August 2010, http://www.defense.gov/releases/release.aspx?releaseid=13782/ (accessed 29 March 2011).
57. Ibid.
58. Bill Lord, e-mail message to author via distribution list, 11 April 2011.
59. M. Bodine Birdwell and Robert Mills. "War Fighting in Cyberspace: Evolving Force Presentation and Command and Control." *Air and Space Power Journal*, Vol XXV, No. 1 (Spring 2011): 26-36.
60. Ibid, 26-36.
61. Chairman, U.S. Joint Chiefs of Staff. *Joint Publication 1: Doctrine for the Armed Forces of the United States*. Washington, DC: CJCS, 2 May 2007 amended through 20 March 2009. http://www.dtic.mil/doctrine/new_pubs/jp1.pdf (accessed 13 April 2011), I-11.
62. Ike Skelton, U.S. Congress. House. *U.S. Cyber Command: Organizing for Cyberspace Operations*. 111th Cong., 2nd sess., 2010. http://democrats.armedservices.house.gov/index.cfm/2010/9/u-s-cyber-command-organizing-for-cyberspace-operations (accessed 7 April 2011).

SELECTED BIBLIOGRAPHY

Birdwell, M. Bodine and Mills, Robert. "War Fighting in Cyberspace: Evolving Force Presentation and Command and Control." *Air and Space Power Journal*, Vol XXV, No. 1 (Spring 2011): 26-36.

Brown, Nancy E. "Difficulties Encountered as We Evolve the Cyber Landscape for the Military," *High Frontier: The Journal for Space & Missile Professions* 5, no. 3 (May 2009), http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf (accessed 3 May 2011).

Clarke, Richard A., and Robert K. Knake. *Cyber War*. New York,NY: HarperCollins Publishers, 2010.

Hollis, David. "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command," *ndu.edu*, **http://www.ndu.edu/press/USCYBERCOM.html** (accessed 23 February 2011).

Joint History Office, Office of the Chairman of the Joint Chiefs of Staff. *The History of the Unified Command Plan 1946-1999*. Washington, DC: Government Printing Office, 2003.

Leigber, William, "Learning to Operate in Cyberspace," Proceedings (February 2011), Vol 137, Iss 2: 32-38. http://www.proquest.com/ (accessed 27 March 2010).

Lopez, C. Todd. "Cyber Command to Unite Network Defense Efforts," *army.mil*, 2 June 2010. http://www.army.mil/-news/2010/06/02/40195-cyber-command-to-unite-network-defense-efforts/ (accessed 4 May 2011).

Lynn, William J, III, "Defending a New Domain," *Foreign Affairs* 89 iss.3 (Sep/Oct 2010): 97-109. http://www.proquest.com/ (accessed 10 April 2011).

U.S. Congress. House. *Terrorism, Unconventional Threats, and Capabilities Subcommittee: Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations*. 111th Cong., 2nd sess., 2010. **http://democrats.armedservices.house.gov/index.cfm/2010/9/terrorism-unconventional-threats-and-capabilities-subcommittee-operating-in-the-digital-domain-organizing-the-military-departments-for-cyber-operations** (accessed 7 April 2011).

_____. House. *2012 Budget Request from U.S. Cyber Command: Hearing before the House Committee of Armed Services Subcommittee on Emerging Threats and*

Capabilities, 112th Cong., 1st sess., 2011, http://armedservices.house.gov/index.cfm/files/serve?File_id=50aeaaff-808b-4f43-a8d0-ad86ec9357f6 (accessed 18 April 2011).

_____. House. *U.S. Cyber Command: Organizing for Cyberspace Operations*. 111th Cong., 2nd sess., 2010. **http://democrats.armedservices.house.gov/index.cfm/2010/9/u-s-cyber-command-organizing-for-cyberspace-operations** (accessed 7 April 2011).

_____. House. *Statement of General C. Robert Kehler Commander United States Strategic Command before the Senate Committee on Armed Services*, 112th Cong., 1st sess., 2011, http://armed-services.senate.gov/statemnt/2011/03%20March/Kehler%2003-29-11.pdf (accessed 3 May 2011).

U.S. Defense Department. "DOD Releases Unified Command Plan 2011." *News Release*, 8 April 2011. http://www.defense.gov/releases/release.aspx?releaseid=14398 (accessed 4 May 2011).

_____. "Sec. Gates Announces Efficiencies Initiatives." *News Release*, 9 August 2010. http://www.defense.gov/releases/release.aspx?releaseid=13782/ (accessed March 29, 2011).

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Publication 1: Doctrine for the Armed Forces of the United States*. Washington, DC: CJCS, 2 May 2007 amended through 20 March 2009. http://www.dtic.mil/doctrine/new_pubs/jp1.pdf (accessed 13 April 2011).

_____. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms.* Washington, DC: CJCS, 8 November 2010 (amended through 31 January 2011. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed 13 April 2011).

_____. *The National Military Strategy of the United States of America 2011: Redefining America's Leadership.* Washington, DC: CJCS, 2011. http://www.jcs.mil/content/files/2011-02/020811084800_2011_NMS_-_08_FEB_2011.pdf (accessed 10 April 2011).

U.S. President. *The National Strategy to Secure Cyberspace*, (Washington, DC: White House, 2003). http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (accessed 10 April 2011).

United States Special Operations Command, "US SOCOM History," http://www.socom.mil/SOCOMHome/Pages/History.aspx (accessed 9 April 2011).

United States Strategic Command, http://www.stratcom.mil/history/ (accessed 2 May 2011).