REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
05-31-2011	FINAL	

4. TITLE AND SUBTITLE

USCYBERCOM: A Centralized Command of Cyberspace

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Stephen M. Rodriguez

Paper Advisor : Jim Nordhill

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

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 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 unprecedented growth of cyberspace and related technologies has impacted nearly every aspect of human society and has opened a new domain where information is communicated more rapidly than ever before. Recognizing the growing potential of cyberspace to impact national security, the Department of Defense (DOD) created the U.S. Cyber Command (USCYBERCOM) in 2010 by merging its offensive and defensive cyber units. But while the concept was to enable a unity of effort under one command, such a centralized command structure challenges the traditional authority that grants Geographic Combatant Commanders (GCC) full control over warfighting efforts in their areas of responsibility (AOR). While there is growing agreement that the nature of defensive cyberwarfare calls for a collective long-term stance and unity of effort, offensive cyberwarfare operations differ in that they are typically targeted within an AOR, short-lived, and distinct to each situation. This raises the question of the GCCs' authority to conduct offensive cyber actions in their respective AORs. However, such authority over offensive cyber operations would mirror the split structure that existed before the creation of USCYBERCOM and counter the intent of unity of effort. Rather, the fundamental characteristics of cyberspace, when fully considered, support the concept of centralized command and control of all warfighting operations in the cyber domain. USCYBERCOM must maintain centralized control of all DOD cyberwarfare efforts and synchronize its efforts through coordination cells embedded with each Combatant Command.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF: UNCLASSIFIED			**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.

USCYBERCOM: A CENTRALIZED COMMAND OF CYBERSPACE

by

Stephen M. Rodriguez

Major, USMC

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:_____

31 May 2011

Contents

Abstract

The unprecedented growth of cyberspace and related technologies has impacted nearly every aspect of human society and has opened a new domain where information is communicated more rapidly than ever before. Recognizing the growing potential of cyberspace to impact national security, the Department of Defense (DOD) created the U.S. Cyber Command (USCYBERCOM) in 2010 by merging its offensive and defensive cyber units. But while the concept was to enable a unity of effort under one command, such a centralized command structure challenges the traditional authority that grants Geographic Combatant Commanders (GCC) full control over warfighting efforts in their areas of responsibility (AOR). While there is growing agreement that the nature of defensive cyberwarfare calls for a collective long-term stance and unity of effort, offensive cyberwarfare operations differ in that they are typically targeted within an AOR, short-lived, and distinct to each situation. This raises the question of the GCCs' authority to conduct offensive cyber actions in their respective AORs. However, such authority over offensive cyber operations would mirror the split structure that existed before the creation of USCYBERCOM and counter the intent of unity of effort. Rather, the fundamental characteristics of cyberspace, when fully considered, support the concept of centralized command and control of all warfighting operations in the cyber domain. USCYBERCOM must maintain centralized control of all DOD cyberwarfare efforts and synchronize its efforts through coordination cells embedded with each Combatant Command.

INTRODUCTION

> ***Cyberspace*** *is 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.*[1]
>
> -U.S. National Military Strategy for Cyberspace Operations

The explosive growth of the internet and its related technologies has been faster than that of any other communication medium in history.[2] In just the past fifteen years, the percentage of internet use across the planet has gone from only 0.4% of the world's total population (16 million users in 1995) to over 30% (two billion users in 2010).[3] This exponential growth clearly demonstrates a dramatically increasing global dependence on the interconnectedness and speed of communications that can only be obtained in cyberspace.

Today nearly every aspect of human society is affected by cyberspace. From business and entertainment, to education and government, connectivity in cyberspace enables enhanced capabilities and near instant response times. But along with these substantial advantages come considerable risks and vulnerabilities since every connection in cyberspace offers a potential opening to those who seek to steal information, corrupt data, or damage systems. This fact, while relevant to every person and organization that communicates in cyberspace, has even more significance to governments that deal with real enemies intent on inflicting real physical damage and harm on its citizens. Militaries, in particular, are increasingly recognizing the potential of activities in cyberspace to impact the operating environment. The United States Department of Defense (DOD), in its 2010 Quadrennial Defense Review Report (QDR) states that "in the 21st century, modern armed forces simply cannot conduct effective high-tempo operations without resilient, reliable information and

[1] (National Military Strategy for Cyberspace Operations 2006, ix)
[2] (Internet Society 2003)
[3] (Internet World Stats n.d.) (Quadrennial Defense Review Report 2010)

communication networks and assured access to cyberspace."[4] The same report estimates that the DOD currently operates more than 15,000 separate computer networks across more than 4,000 military installations in 88 countries.[5] Being so vast and widespread, these DOD networks have increasingly become prime targets for adversaries that strive to challenge U.S. military power without the need for traditional forms of confrontation.

In response to this rapidly growing threat, and in an effort to organize and standardize cyber practices and operations, the DOD, in May 2010, created the U.S. Cyber Command (USCYBERCOM or CYBERCOM).[6] This new command was established to "synchronize and coordinate cyber-warfighting effects across the global security environment."[7] However, while sound in concept and simple in theory, the difficult question that arises is how to best Command and Control (C2) warfighting operations in cyberspace while dealing with the inevitable real-world C2 issues that can hinder CYBERCOM's ability to most effectively manage cyberwarfare efforts. To address this issue, three overarching characteristics of cyberspace must be considered: first is the borderless nature of cyberspace and its ability to simultaneously affect different geographic Areas of Responsibility (AOR), second is the speed of cyber events and the associated response times, and third is the vast scope of and rate of growth of cyberspace. Once these factors are thoroughly examined, it becomes clear that in order to most effectively address the unique opportunities and vulnerabilities that the domain of cyberspace offers, USCYBERCOM must maintain fully centralized control of all DOD cyberwarfare efforts and synchronize its efforts through coordination cells embedded with each Combatant Command.

[4] (Quadrennial Defense Review Report, ix)
[5] (Quadrennial Defense Review Report, 37)
[6] (Barkley 2010, 5)
[7] (Gates 2009)

BACKGROUND: Telegraph to Cyberwar

All I knew about the word "cyberspace" when I coined it, was that it seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page.[8]

-William Gibson

The reality of cyberspace existed long before it was recognized as such. By definition, cyberspace itself was born with the introduction of the first electric telegraph in the 1830s, which evolved over the next century and a half into radio wave transmissions of voice and data over wire and through the air.[9] The actual notion of cyberspace, though, wasn't introduced until 1984 when William Gibson used the term in his novel, *Neuromancer*, where he describes cyberspace as "a consensual hallucination…a graphic representation of data abstracted from banks of every computer in the human system…unthinkable complexity."[10] Certainly no one at the time could have foretold the significance that the word would come to represent. Just three decades later, cyberspace has evolved into not only the most widely used and rapidly growing information exchange medium that the world has ever known, but it is also now being generally accepted as a domain of its own.[11]

Militarily, cyber-operations are not a new concept. In 1982 a U.S. satellite detected an immense blast and fire in the middle of Siberia. At first thought to be the result of a small nuclear device, it was soon determined to be an accident in a Soviet natural gas pipeline. The cause was a malfunction in the pipeline's pressure monitoring system resulting from a computer virus, or 'logic bomb', which had been inserted into the pipeline's computer controlled management system. This virus caused the pipeline's pumps and valves to

[8] (Gibson, No Maps for These Territories 2000)
[9] (White n.d.)
[10] (Gibson, Neuromancer, 128)
[11] (Internet Society 2003)

malfunction, leading to pressures in the system that caused one of the most "monumental non-nuclear explosions ever seen from space."[12] While the computer virus in that case was not inserted via the Internet (it had actually been inserted at the software supplier's site), it is considered by many to be the first significant instance of a cyber-attack. Since then, cyberspace capabilities have had a great impact on, and are now an integral part of, the conduct of all of the doctrinal warfighting functions. Today's military commanders rely "almost exclusively on technologies in cyberspace to move information to decision makers, commanders, and troops giving combatant commanders unparalleled abilities to observe, orient, decide and act."[13] Cyberspace is now widely considered an actual domain of military operations which many are considering the "fifth realm of warfare, complementing air, land, sea and space as the realms that battles will be conducted in into the future."[14] Recognition of this role that cyberspace activities will play in the future security of the nation was the motivation behind the reorganization that aimed to synchronize, coordinate, and streamline DOD cyber capabilities through the creation of USCYBERCOM.[15]

Prior to the establishment of USCYBERCOM in May 2010, DOD cyberwarfare capabilities were divided among organizations and service components. In essence, the main division was between the offensive and defensive cyber capabilities of the armed forces.[16] On the offensive side, Joint Functional Component Command-Network Warfare (JFCC-NW) had responsibility for planning and executing operations "in and through cyberspace to assure U.S. and allied freedom of action, denying adversaries' freedom of action, and enabling effects beyond the cyber domain." This organization, a subordinate command to

[12] (War in the Fifth Domain 2010)
[13] (Franklin 2010, 2)
[14] (Jongsma 2008)
[15] (DOD Fact Sheet on U.S. Cyber Command 2010)
[16] (Alexander, Speech at the Cybersecurity Policy Debate Series 2010)

U.S. Strategic Command (STRATCOM), was commanded by the director of the National Security Agency (NSA) and collocated with NSA at Ft Meade MD.[17] On the defense side, Joint Task Force-Global Network Operations (JTF-GNO) had the responsibility for "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 the DOD's full spectrum of warfighting, intelligence, and business missions," or in short, to manage the DOD networks and to defend them from outside attacks.[18] This unit was also structurally a subordinate command of STRATCOM, but was commanded by the Director of the Defense Information Systems Agency (DISA) and located at DISA headquarters in Arlington, VA.[19] While these two commands were both officially under STRATCOM, they were organizationally and geographically divided which, considering the time criticality of decision making and of synchronizing efforts in cyberspace, made unified action and effective coordination difficult to achieve. This was the driving force behind the decision to merge the two DOD cyber units into a single command in the forming of USCYBERCOM.[20]

U.S. CYBER COMMAND: Merging Cyber Capabilities

> *Until recently, the military's cyber effort was run by a loose confederation of joint task forces spread too far and too wide, both geographically and institutionally, to be fully effective.*[21]
>
> -Deputy Secretary of Defense William J. Lynn

The United States Cyber Command was officially established on May 21, 2010, as a Subordinate Unified Command to STRATCOM. Staffed by 464 military personnel and 476 civilians, most coming from the staffs of the two legacy organizations that were merged,

[17] (Hanson 2009, 4)
[18] (Barkley 2010, 8)
[19] (Alexander, Speech at the Cybersecurity Policy Debate Series 2010)
[20] (Barkley 2010, 9-10)
[21] (Lynn, Speech at the STRATCOM Cyber Symposium 2010)

CYBERCOM was charged with "pulling together existing cyberspace resources, creating synergy that does not currently exist and synchronizing war-fighting effects to defend the information security environment."[22] In his establishing memorandum on June 23, 2009, Secretary of Defense Robert Gates directed the Commander of STRATCOM to "delegate authority to conduct the specified cyberspace operations detailed in Section 18.d.(3) of the Unified Command Plan (UCP) to the Commander, USCYBERCOM." The same memorandum then went on to direct that "combatant commanders, Services, and DoD agencies remain responsible for compliance with USSTRATCOM's direction, as stipulated by USCYBERCOM, for operation and defense of the Global Information Grid."[23] Although the classified status of the UCP precludes stating the precise details of Section 18.d.(3), Secretary Gate's mandate was clear: CYBERCOM will have authority over all DOD cyber operations while all other DOD entities must comply with CYBERCOM's directives.[24]

At the same time, as is often the case, the simplicity of such clear direction can be clouded by real-world issues. While the character of cyberspace seems to dictate the need for a truly centralized command model, any adversaries fighting in cyberspace will physically exist and operate in the Geographic Combatant Commanders' (GCCs) AORs. This raises potential for issues if the GCC is being directed to concede authority over such individuals and/or their equipment to USCYBERCOM. This kind of unconventional C2 structure "challenges the traditional authorities exercised by GCCs and will likely create friction points in future command relationship definition with USCYBERCOM."[25] Hence this is a major challenge that must be reconciled, since employing such a centralized approach to C2 in this

[22] (Alexander, Posture Statement on Emerging Threats , 4) (DOD Fact Sheet on U.S. Cyber Command 2010)
[23] (Gates 2009)
[24] (Crowell 2010, 7)
[25] (Franklin 2010, 4)

type of situation seems most logical, but at the same time might impede a GCCs ability to fully control his AOR. Finding the most effective solution to this issue is critical to maintaining a competitive advantage over enemies that aren't always as constrained by the same bureaucratic, legal, and hierarchical processes that commonly impede western democratic government processes.

CHARACTERISTICS OF CYBERSPACE

> *The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had.*[26]
>
> -Eric Schmidt

There are three overarching characteristics of cyberspace that merit consideration in determining the most appropriate command and control structure for CYBERCOM to assert over DOD cyberwarfare efforts: the borderless nature of cyberspace and its ability to simultaneously affect different geographic AORs, the speed of cyber events and associated response times, and the vast scope of and projected rate of growth of cyberspace. These three areas rate further examination to determine the validity of the rationale for fully centralized control.

Borderless:

The nature of cyberspace is inherently complex and difficult to comprehend. Often described as virtual, conceptual, or a notional environment, it seems to be something that human beings generally consider to be an imaginary realm.[27] In reality though, cyberspace can in fact be defined in physical terms when considering its true nature. Cyberspace exists only in and on those physical objects that are interconnected to all the other physical objects

[26] Eric Schmidt, CEO of Google 2001-2011, in a speech at the JavaOne conference, April 1997
[27] (Asymetricthreat.net glossary)

that 'contain' cyberspace. Without the computer systems, processors, storage devices, transmission equipment, wires, cables, and other media used to connect them, cyberspace would cease to exist. At the same time, while the aforementioned equipment that makeup cyberspace are all physical objects that exist in real locations, the actual transmissions of data that link them all are composed only of energy which pays little heed to the man-made borders or boundaries of the 'real' world. Wherever an energy transmission of data can go, (whether by wire, cable, or through the air) cyberspace will be extended so long as there is a physical piece of equipment on the other end that can process the transmission. Furthermore, the actual method of transmission that is used in cyberspace is typically one of packet switching, which in essence breaks up the 'message' into smaller pieces of data, which are then transmitted to the destination via many different physical routes along different transmission media. This data is reassembled into the original message only upon reaching its physical destination.[28] In essence, a typical transmission of data through cyberspace will likely pass physically through multiple AORs regardless of its point of origin or destination. Cyberspace truly has no boundaries, confines, or borders, and can be extended anywhere that the physical network architecture can be extended.

This borderless aspect of cyberspace presents complications for any attempt to control actions in it. Cyber-actions at one location in a particular AOR may be 'aimed' at a target in the same or another AOR, while at the same time, the transmission of data will undoubtedly pass through additional AORs in the process. Moreover, once released, the transmission of data often cannot be recalled and the effect of the transmission after reaching its target may not be controllable. "Second and third order effects resulting from cyber

[28] Transmissions in cyberspace follow the TCP/IP protocol, which uses packet switching of data to transmit and receive messages; (Microsoft TechNet 2003)

attacks on untargeted systems are sometimes impossible to anticipate or counter" and very likely may impact unintended victims.[29] Examples of the capacity of computer attacks to spread unchecked abound in the very short history of the Internet. One of the first occurrences of such an attack occurred in 1988 when a Cornell University graduate student named Robert Morris designed a program that was intended as an experiment to measure the size of the Internet.[30] However, this program quickly ended up replicating itself and spreading at an unexpected and massive rate, and Morris found himself being credited with (and subsequently convicted of) creating the internet's first worm.[31] More recently in 2001, the NIMDA virus (ADMIN spelled backwards) demonstrated the technical advances being seen in cyber attacks. NIMDA, which was actually a combination of a computer virus and a computer worm, spread with tremendous speed and used multiple methods to attempt to infect computer systems until it found one that gave it access. "It went from nonexistent to nationwide in an hour, lasted for days," and quickly became the most widespread virus in the world "attacking tens of thousands of servers and hundreds of thousands of PCs."[32]

While these two previous examples clearly demonstrate the tendency of such non-targeted cyber attacks to spread without regard for geographic borders or boundaries, a more pertinent example of a targeted cyber attack simultaneously impacting multiple AORs can be seen in the 2008 Russo-Georgian War. During that conflict, Russian entities launched offensive denial-of-service operations against Georgian military, government, and civilian websites to disrupt Georgian C2 capabilities and to create unrest in the civilian population.[33]

---

[29] (Franklin 2010, 4-5)
[30] (Harris 2009)
[31] Despite claiming no intention to cause harm, Morris was convicted of unauthorized access to a "federal interest computer" in 1990; (PBS.org Notable Hacks n.d.)
[32] (The National Strategy to Secure Cyberspace 2003) (Thorsberg 2002).
[33] (Haddick 2011)

During this, in a successful effort to mask the true points of origin of the attacks, the Russian entities routed their efforts through a variety of third-party servers around the globe. One such instance of particular note involved a website "hosted by a company in Texas that was used to attack a Georgian government website that had been relocated – coincidentally – to a web hosting company in Atlanta, Georgia. In essence, the United States experienced collateral damage during these cyber attacks."[34]

Clearly, these examples highlight how the borderless aspect of cyberspace can lead to a simultaneous impact on multiple AORs, not only from the arbitrary routing of data across the numerous pathways of the Internet, but also from intentional manipulation of those same pathways. As stated by General Keith Alexander, Commander of USCYBERCOM, just this past March, "The lack of geographic borders in cyberspace means that a threat to one can be a threat to all, which gives us a real incentive to share situational awareness and best practices that help to protect our military, government, and private networks and data."[35] Centralized command of DOD cyberwarfare efforts would be the best way to negate those threats that capitalize on the lack of borders and boundaries in cyberspace.

Speed:

In addition to the borderless aspect of cyberspace supporting the need for centralized control of DOD cyberwarfare efforts, the characteristic of speed also support this need. There is no question that actions in cyberspace occur quickly; in fact so quickly that the term 'net-speed' is becoming a common colloquialism. This extraordinary speed of actions in cyberspace is related not only to the fact that the actual transport of data across the different transmission media occurs at near light speed, but also to the capability of the digital

[34] (Korns 2009, 97)
[35] (Alexander, Posture Statement to the Subcommittee on Emerging Threats and Capabilities 2011, 15)

equipment to process and store the data, which has been increasing exponentially over the past decades, in accordance with Moore's Law.[36] This incredible speed of digital equipment was critical in the case of the NIMDA virus that was highlighted previously. While the worldwide scope of the virus was alarming, even more astonishing was the speed at which the virus was able to spread itself. It took only 22 minutes from introduction into the Internet for it to become the most widespread virus in the world.[37]

For a clear picture of the incredible rate of growth in the capabilities of the military's digital communication equipment, one needs only to compare the capabilities during the two Iraqi conflicts of the past two decades. "Reportedly, a message that took more than an hour to send in 1991 takes less than a second today."[38] Such a simple example of the incredible progress in transmission capabilities over just the past two decades, hints at the potential progress in these capabilities that will be seen in the future.

There is common agreement among cyber-professionals that offensive cyberwarfare has an edge over defensive cyberwarfare.[39] Many of the characteristics of the Internet favor the cyber attacker, including "worldwide connectivity, vulnerable network infrastructure, poor attacker attribution, and the ability to choose their time and place of the attack."[40] These advantages, because of the almost anti-security character of the Internet, give an attacker a definite advantage over the defender. Deputy Secretary of Defense, William Lynn, addressed this issue in an article published in the September 2010 edition of Foreign Affairs, when he stated: "the internet was designed to be collaborative and rapidly expandable and to

[36] Moore's Law predicts that the number of transistors on a microchip double every one to two years, which results in a corresponding increase in the processing power of digital equipment; (Kanellos 2005)
[37] (Thorsberg 2002)
[38] (Vego 2007, III-69)
[39] (Hollis, USCYBERCOM: The Need for a Combatant Command versus a Subunified Command 2010, 49)
[40] (Geers 2011, 7-8)

have low barriers to technological innovation; security and identity management were low priorities. For these structural reasons, the U.S. government's ability to defend its networks always lags behind its adversaries' ability to exploit U.S. networks' weaknesses."[41] Secretary Lynn's assessment highlights the inherent nature of the Internet away from security, however, he also brings to light the one factor that most enables all of the defenders efforts: speed.

The effectiveness of an attack will be determined largely by the speed of the response on the part of the defender. Any advantages that the attacker has only matter if combined with sufficient speed to outpace the defenders ability to effectively deploy his defense. On this matter, Secretary Lynn went on to say, "Cyberwarfare is like maneuver warfare, in that speed and agility matter most."[42] General Alexander expressed a similar thought on the criticality of speed when he said, "we must be able to operate and adapt to situations at net speed, leveraging technology for automated, autonomous decision-making."[43] This statement agrees with Secretary Lynn's comment, but also touches on the true enemy of speed in the cyber environment: human input. In suggesting the need for "automated, autonomous decision-making", General Alexander was in reality expressing the need to eliminate layers of human interaction and decision making. The speed of events in cyberspace allow no time for the typical layers of human engagement that are involved with decision making in the physical domains, such as the relative importance of a threat, which course of action would be best, or even who is in charge of a particular situation. Only by eliminating those layers through such automated pre-determined courses of action, as General Alexander suggests, will the DOD be able to keep pace with the threat. Centralized

[41] (Lynn, Defending a New Domain 2010)
[42] (Lynn, Defending a New Domain 2010)
[43] (Alexander, Speech at the Cybersecurity Policy Debate Series 2010)

control of DOD cyberwarfare efforts is the best way to minimize the layers of human interaction and decision making.

Scope:

The significance of cyberspace today and in the future can't be overstated. As detailed earlier, the scope and rate of growth of cyberspace has greatly outpaced all other communication technologies of the past. Just recently passing two billion internet users, this number is forecast to approach three billion world-wide by 2015.[44] As the number of users increases and the capacity of equipment to transmit and receive data grows, so does the 'size' of cyberspace. For USCYBERCOM, this translates into both more capabilities and more vulnerabilities to protect. But it also offers more opportunity to capitalize on the leveraging power that can be gained by maximizing unity of effort through unity of command.

Already a shortage of resources and proficiency to both operate and to maintain the growing cyber infrastructure is impacting the integrity and security of DOD networks. Poor oversight of network resources commonly leads to avoidable vulnerabilities, such as unapplied software patches, unattended firewalls, and un-updated antivirus software.[45] General Alexander expressed concern for this issue in March 2011 in his posture statement to the House Subcommittee on Emerging Threats and Capabilities when he stated: "We are finding that we do not have the capacity to do everything that we need to accomplish. To put it bluntly, we are very thin, and a crisis would quickly stress our cyber forces."[46] This kind of shortcoming in resources points toward the benefits that could be gained from centralizing cyberwarfare C2 in order to maximize unity of effort of all DOD cyber forces and to minimize waste through eliminating duplicate capabilities, systems, training, and efforts.

[44] (Internet Use Forecast by Country n.d.)
[45] (Alexander, Posture Statement to the Subcommittee on Emerging Threats and Capabilities, 7)
[46] (Alexander, Posture Statement to the Subcommittee on Emerging Threats and Capabilities, 16)

Additionally, due to the constant evolution in cyber capabilities, the need to keep pace with cutting-edge technology creates an immense financial expense for equipment acquisitions, updates, and related training. Centralized C2 would allow CYBERCOM and DOD to benefit from economies of scale in acquisitions, training, and execution, particularly if combined with other government initiatives for common programs. An example of the potential of such a leveraged acquisition arrangement can be seen in a recent case where multiple contracts were awarded for the purchase of government encryption products involving a group of twenty DOD components and over twenty other government agencies. "This initiative was the first (and only) true effort to leverage the entire government to achieve huge product discounts, often 90 percent to 98 percent lower than previous GSA pricing."[47] Such a clear example of the benefits that can be gained from consolidating acquisition activities demonstrates yet another potential advantage to centralizing the command and control of DOD cyberwarfare efforts.

COUNTER POINT: Decentralized Offensive C2

> *We must be able to operate and adapt to situations at net speed, leveraging technology for automated, autonomous decision-making.*
>
> -General Keith Alexander, CDR USCYBERCOM

While the concept of centralized command and control offers many potential benefits as discussed above, some would argue that this is not the optimal way to manage the military's cyberwarfare efforts into the future. Rather, while there is growing agreement that the nature of defensive cyber operations supports a centralized control model, offensive cyber operations don't garner such sentiment. Where defense of the overall DOD network calls for a collective long-term stance and unity of effort, offensive operations differ in that

[47] (Hollis, Cyber Defense: U.S. Cybersecurity Must-Do's 2011, 18-19)

such actions are most often targeted, short-lived, and distinct to each particular situation. The targets of such attacks physically exist at some geographic location and therefore fall within a GCC's AOR. This leads to the argument that GCC's are better positioned to recognize and understand the distinctness and unique needs of each situation, and therefore should have the ultimate authority to decide on offensive cyberwarfare efforts in their AOR's. Additionally, as cyber weapons evolve, the improved capabilities of such weapons will allow better control to reduce secondary effects that may spread to other AORs. Such sophistication was recently seen in the Stuxnet virus that targeted Iran's nuclear program. This "groundbreaking piece of malware" was created to target the control systems at Iran's uranium enrichment facilities while limiting collateral effects. It was designed specifically to "limit the spread… so that it would stay within the targeted facility."[48] The resultant effects of this sophisticated virus seem to have fulfilled its purpose as it "reportedly set back the nation's nuclear program by as much as several years" with no reports of significant secondary damage.[49] Such effectiveness and controllability in a cyber weapon today indicates that cyber weapons will continue to evolve to allow even more control in the future, further supporting a GCC's right for authority over offensive cyber actions in his AOR.

While the above arguments hold merit, the need for a global coordination of offensive cyber efforts remains. Despite the fact that GCC's clearly are best positioned to recognize the unique aspects and needs of situations in their AORs, the nature of the cyber domain demands a level of synchronization that can only come from a centralized control. Complex weapons, such as Stuxnet, involve a significant investment of time and resources to develop, but have a very short effective life (usually one-time use) since adversaries quickly adapt and

[48] (Keizer 2010)
[49] (Stuxnet Propmts Iran to Recruit Cyber Warriors 2011)

create defenses once the weapon is employed.[50] Further, while future advances in the development of cyber weapons will likely provide increasing improvements in control over unintentional effects, the borderless aspect of cyber operations remains relevant since the Internet's arbitrary routing methods of data transmission cannot be avoided nor ignored.

The division of cyberwarfare efforts that would result from granting GCCs authority over offensive cyber operations mirrors the split structure that was in place prior to the creation of USCYBERCOM, which has already been recognized as sub-optimal. Regressing back to such a C2 structure would defy the intent of the creation of USCYBERCOM and would negate the benefits of merging DOD's offensive and defensive cyber organizations. CYBERCOM must maintain centralized control of all DOD cyberwarfare efforts, both offensive and defensive.

CONCLUSION AND RECOMMENDATIONS

> *The key part of Cyber Command is the linking of intelligence, offense and defense under one roof.*
>
> -Deputy Secretary of Defense William J. Lynn

The unprecedented growth of cyberspace impacts nearly every aspect of human society and has opened a new domain where information is communicated faster than ever before. Recognizing the growing potential of cyberspace to impact national security, the DOD created USCYBERCOM in order to "synchronize and coordinate cyber-warfighting effects."[51] But while the concept was to ensure unity of cyber effort under one command, this challenges the traditional command structure that grants GCCs full authority for war-fighting efforts in their AORs. However, once the fundamental characteristics of cyberspace

[50] (Geers 2011, 13)
[51] (Gates 2009)

are considered, it becomes clear that deviation from this conventional authority model is not only warranted, but is necessary to maintain an advantage over adversaries in cyberspace. To this end, the following three recommendations are offered:

USCYBERCOM must maintain centralized control of all U.S. warfighting operations in cyberspace, both offensive and defensive. To meet the needs of the other Combatant Commands, especially the GCCs, coordination cells should be physically embedded within each COCOM headquarters in order to synchronize CYBERCOM efforts in the cyber domain with GCC operations in the traditional warfighting domains. These coordination cells must remain under CYBERCOM's command, but with DIRLAUTH to the CCDRs.

USCYBERCOM should be developed into a full Combatant Command. Establishing CYBERCOM as a subunified command rather that a COCOM was due in large part to time and effort required to develop a full COCOM. "The reduced up front effort to develop a subunified command…more quickly achieve[d] DOD's immediate goal of a unified full-spectrum Cyberwar capability…but with a reduced structure, mission, and authority compared to a full unified COCOM."[52] While the commander of STRATCOM has delegated the authority to conduct cyberwarfare operations to the commander of USCYBERCOM, a level of legitimacy and influence equal to that of the GCC's will only be achieved by attaining CCDR status equal to that of the GCC's.

USCYBERCOM should be given acquisition authority, similar to that of U.S. Special Operations Command. This will enable CYBERCOM to "unify and streamline the procurement of military cyberspace capabilities," and to take advantage of the leveraging power of military-wide purchasing.[53]

[52] (Hollis, USCYBERCOM: The Need for a Combatant Command versus a Subunified Command 2010, 49)
[53] (Hollis, USCYBERCOM: The Need for a Combatant Command versus a Subunified Command 2010, 51)

Bibliography

Alexander, Keith B. "Posture Statement to the House Armed Services Subcommittee on Emerging Threats and Capabilities." Washington, DC, March 16, 2011.

—. "Speech at the Center for Strategic and International Studies Cybersecurity Policy Debate Series." *U.S. Cybersecurity Policy and the Role of U.S. Cybercom.* Washington, D.C., June 3, 2010.

Asymetricthreat.net glossary. n.d. http://asymmetricthreat.net/glossary.shtml (accessed April 21, 2011).

Barkley, James. *Interagency Coordination @ Net Speed: Recommendations to Maximize Interagency Coordination and Capabilities at US CYBERCOM.* Harvard University Kennedy School, 2010.

Crowell, Richard M. "War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare." Newport: U.S. Naval War College, January 2010.

DOD Fact Sheet on U.S. Cyber Command. Washington, DC: U.S. Department of Defense, 2010.

Franklin, David M. *U.S. Command Relationships in the Conduct of Cyber Warfare: Establishment, exercise, and Institutionalization of Cyber Coordinating Authority.* Newport: Naval War College, 2010.

Gates, Robert. "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations." Washington, DC, June 23, 2009.

Geers, Kenneth. *Sun-Tzu and Cyber War.* Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2011.

Gibson, William. *Neuromancer.* New York: Berkley Publishing Group, 1989.

Gibson, William. *No Maps for These Territories* (2000).

Haddick, Robert. "This Week at War: Lessons from Cyberwar I." *Foreign Policy*, January 28, 2011.

Hanson, Kraig. *Organization of DoD Computer Network Defense, Exploitation, and Attack Forces.* Carlisle Barracks, PA: U.S. Army War College, 2009.

Harris, Shane. "The Cyberwar Plan." *National Journal*, November 13, 2009.

Hollis, David M. "Cyber Defense: U.S. Cybersecurity Must-Do's." *Armed Forces Journal*, March 2011.

—. "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command." *Joint Forces Quarterly*, 3d Quarter 2010.

Internet Society. "intgovforum.org." *The Genius of the Internet: Open Processes Drive Growth and Connectivity.* October 11, 2003. http://www.intgovforum.org/Substantive_1st_IGF/isocnews-4.pdf (accessed April 8, 2011).

Internet Use Forecast by Country. n.d. http://www.etforecasts.com/products/ES_intusersv2.htm (accessed April 12, 2011).

Internet World Stats. n.d. http://www.internetworldstats.com/emarketing.htm (accessed April 10, 2011).

Jongsma, Carl. *USAF: Cyberspace represents a fifth, costly, realm of warfare.* September 11, 2008. http://www.techworld.com.au/article/260027/usaf_cyberspace_represents_fifth_costly_realm_warfare/ (accessed April 7, 2011).

Kanellos, Michael. "New Life for Moore's Law." *Cnet News.* April 19, 2005. http://news.cnet.com/New-life-for-Moores-Law/2009-1006_3-5672485.html (accessed April 27, 2011).

Keizer, Gregg. "Is Stuxnet the 'best' malware ever?" *computerworld.com.* September 16, 2010. http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever_ (accessed April 9, 2011).

Korns, Stephen W. "Cyber Operations: The New Balance." *Joint Forces Quarterly*, 3d Quarter 2009.

Lynn, William J. "Defending a New Domain." *Foreign Affairs*, September/October 2010.

—. "Speech at the STRATCOM Cyber Symposium." Omaha, May 26, 2010.

Microsoft TechNet. March 28, 2003. http://technet.microsoft.com/en-us/library/cc786128(WS.10).aspx (accessed April 18, 2011).

National Military Strategy for Cyberspace Operations. Washington, DC: United States Office of the Chairman of the Joint Chiefs of Staff, 2006.

PBS.org Notable Hacks. n.d. http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/notable.html (accessed April 21, 2011).

Quadrennial Defense Review Report. Washington, DC: U.S. Department of Defense, 2010.

Stuxnet Propmts Iran to Recruit Cyber Warriors. March 15, 2011. https://www.infosecisland.com/blogview/12562-Stuxnet-Prompts-Iran-to-Recruit-Cyber-Warriors.html (accessed March 22, 2011).

The Economist. "War in the Fifth Domain." July 1, 2010.

The National Strategy to Secure Cyberspace. Washington, DC: U.S. Department of Homeland Security, 2003.

Thorsberg, Frank. "The World's Worst Viruses." *pcworld.com.* August 23, 2002. http://www.pcworld.com/article/103992/the_worlds_worst_viruses.html (accessed April 10, 2011).

Tritz, Gerald L. *Cyberspace and the Operational Commander.* Newport, RI: U.S. Naval War College, 2010.

Vego, Milan N. *Joint Operational Warfare: Theory and Practice.* Newport: U.S. Naval War College, 2007.

White, Thomas H. *United States Early Radio History.* n.d. http://earlyradiohistory.us/sec002.htm (accessed April 16, 2011).