# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 05-18-2015 | FINAL | |

**4. TITLE AND SUBTITLE**

**Beyond Mission Command: Maneuver Warfare for Cyber Command and Control**

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**

**Maj Wilson R. McGraw, USMC**

Paper Advisor (if Any): Professor Richard M. Crowell

**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.
Reference: DOD Directive 5230.24

**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 rapidly expanding and dynamic nature of the cyber domain requires that U.S. Cyber Command adopts maneuver warfare's decentralized command and control doctrine to maximize military cyberspace operations. Since the establishment of U.S. Cyber Command in 2009, cyberspace operations have increasingly gained visibility across the U.S. government and DoD in particular. In that time, a centralized command and control structure has evolved to globally control military cyberspace operations from U.S. Cyber Command, vice delegating cyber forces and authorities to combatant commanders and below. Decentralized command and control will allow U.S. cyber forces to take advantage of tactical innovation in this emerging domain, to better allow for operational objective accomplishment by combatant and joint force commanders, and to succeed during cyberspace operation in an A2AD environment.

**15. SUBJECT TERMS**

**command and control; maneuver warfare; cyberspace; cyberspace operations; cyber warfare, mission command; decentralization**

| 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 | | 26 | 19b. TELEPHONE NUMBER *(include area code)* 401-841-3556 |

**Standard Form 298 (Rev. 8-98)**

**NAVAL WAR COLLEGE**
**Newport, R.I.**

# Beyond Mission Command: Maneuver Warfare for Cyber Command and Control

**by**

**Wilson R. McGraw**

**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: _____**

**18 May 2015**

## Contents

## Paper Abstract

*Beyond Mission Command: Maneuver Warfare for Cyberspace Command and Control*

The rapidly expanding and dynamic nature of the cyber domain requires that U.S. Cyber Command adopts maneuver warfare's decentralized command and control doctrine to maximize military cyberspace operations. Since the establishment of U.S. Cyber Command in 2009, cyberspace operations have increasingly gained visibility across the U.S. government and the Department of Defense in particular. In that time, a centralized command and control structure has evolved to globally control military cyberspace operations from U.S. Cyber Command, vice delegating cyber forces and authorities to combatant commanders and below. Decentralized command and control will allow U.S. cyber forces to take advantage of tactical innovation in this emerging domain, to better allow for operational objective accomplishment by combatant and joint force commanders, and to succeed during cyberspace operation in an A2AD environment.

Cyberspace[1] and its associated technologies offer unprecedented opportunities to the United States and are vital to our Nation's security and, by extension, to all aspects of military operations. –Robert M. Gates, Secretary of Defense[2]

## INTRODUCTION

*"Unbelievable," thought the team leader of special operations forces team 2835. During a supporting reconnaissance mission, team 2835 observed the #1 high value individual (HVI) enter their target building. The building was not only known to be heavily booby trapped, but was full of innocent women and children. The team leader came up with a plan that would utilize a high tech cyber tool to lure the HVI outside where he could be quietly captured. All modes of communication to higher headquarters were not working to get approval for the cyberspace operation. The team's frustration turned to failure when an enemy convoy arrived to escort the HVI safely away under heavy guard. Team 2835 had higher headquarters' objective within their grasp, and could only think, "There has got to be a better way to avoid missing these kinds of opportunities."*

This fictional scenario highlights how centralized command and control of cyberspace operations down to the tactical level can cause failure to achieve an operational objective and have negative strategic effects for the security of the United States (U.S.). Centralization is contrary to maneuver warfare's command and control philosophy of using mission tactics, where decentralization is the key to operating in an uncertain, disorderly, and fluid environment.[3] Decentralization of command and control has proven successful across the range of military operations since the U.S. Marine Corps adopted maneuver warfare doctrine in 1989.

Based on Chairman of the Joint Chiefs of Staff General Dempsey's *Mission Command* white paper, decentralized execution through mission-type orders, has recently received high levels of visibility.[4] However, maneuver warfare's command and control philosophy calls for

---

[1] Cyberspace: A global domain within the information environment consisting of the interdependent networks of information technology infrastructure and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (JP 3-12R, *Cyberspace Operations*, 5 Feb 2013).
[2] Robert M. Gates, U.S. Secretary of Defense, *Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations*, Memorandum for the Secretaries of the Military Departments, et al. (Washington DC: SECDEF, 23 June 2009), 1.
[3] U.S. Marine Corps, *Warfighting*, Marine Corps Doctrinal Publication (MCDP) 1 (Washington, DC: Headquarters U.S. Marine Corps, 1997), 78.
[4] Chairman, U.S. Joint Chiefs of Staff, *Mission Command*, (Washington, DC: CJCS, 3 April 2012).

greater decentralization than mission command. Secretary Gates accurately assessed the opportunities that cyberspace offers for our military operations and national security.[5] These opportunities can only be realized by the U.S. military establishing a command and control structure that enables military effectiveness in cyberspace, just as it has in the physical domains.[6] Maneuver warfare's decentralized command and control doctrine should be adopted to maximize U.S. military operations in cyberspace.

## BACKGROUND

Maneuver warfare doctrine acknowledges war's natural features of friction, uncertainty, fluidity, and disorder.[7] It seeks to allow successful military operations by negating these influences on friendly forces and taking advantage of or creating their effects on the enemy. Each individual is affected and the collective accumulation of the effects can weaken a unit as a fighting force. Weakening can also take place when commanders are overwhelmed by these known features of warfare and translate their individual state into inaction on the part of their forces. Maneuver warfare seeks to take advantage of war's nature by decentralizing command and control such that subordinate commanders take the initiative in decision making based on senior's intent, without passing information up the chain of command for approval.[8]

While sharing many elements with maneuver warfare, mission command's decentralization of execution through the use of mission-type orders is a more centralized form

---

[5] Robert M. Gates, U.S. Secretary of Defense, *Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations*, Memorandum for the Secretaries of the Military Departments, et al. (Washington DC: SECDEF, 23 June 2009), 1.
[6] Col. David C. Hathaway, *The Digital Kasserine Pass: The Battle Over Command and Control of DoD's Cyber Forces* (21st Century Defense Initiative Policy Paper, Foreign Policy at Brookings: Brookings Institute, 15 July 2011), Accessed 20 April, 2015. http://www.brookings.edu/~/media/research/files/papers/2011/7/15%20cyber%20forces%20hathaway/0715_cyber_forces_hathaway.pdf, 2.
[7] U.S. Marine Corps, *Warfighting*, Marine Corps Doctrinal Publication (MCDP) 1 (Washington, DC: Headquarters U.S. Marine Corps, 1997), 19.
[8] Ibid, 78.

of operating.[9] As a philosophy, mission command allows too much centralization of command and control while guarding against micromanagement by only telling a subordinate what to accomplish but not how they should do it. Mission command seeks to mitigate the rapidly changing nature of the operating environment, while maneuver warfare's philosophy strives to breed warfighters that not only thrive in, but help create rapid change and uncertainty.[10]

Cyberspace, where global action can take place at the speed of light, may be the most dynamic and uncertain of the warfighting domains. The fluidity of cyberspace is exemplified by Moore's Law that states that every two years the processing power of computers will double.[11] Even though it is a man-made domain, cyberspace is not simply a network of connected hardware and software. Joint doctrine describes it as three layers: a physical network, a logical network, and a cyber-persona.[12] Cyberspace is often only taken at the face value of the physical and logical layers, even though it is the human element of the cyber-persona that creates the most complexity. The scientific, zeros and ones foundation of computer systems may lead people to think that every action in cyberspace can be cataloged, categorized, and known, however computer systems are not good at identifying human intentions. As cyberspace technology continues to advance, civilian life and military operations only become more dependent on the domain.[13]

---

[9] Chairman, U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication (JP) 3-0 (Washington DC: CJCS, 11 August 2011), II-2.
[10] U.S. Marine Corps, *Warfighting*, Marine Corps Doctrinal Publication (MCDP) 1 (Washington, DC: Headquarters U.S. Marine Corps, 1997), 80.
[11] *Moore's Law or How Overall Processing Power for Computers will Double Every Two Years*, accessed 21 April 2015, http://www.mooreslaw.org/.
[12] Chairman, U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication (JP) 3-12R (Washington, DC: CJCS, 5 February 2013), I-2.
[13] Richard M. Crowell, *Some Principles of Cyber Warfare (NWC 2160)* (U.S. Naval War College, Joint Military Operations Department, Newport, RI: U.S. Naval War College, January 2015), 5.

Cyberspace gained attention as a warfighting domain in 2009 when the Department of Defense (DOD) established U.S. Cyber Command as a subordinate unified command within U.S. Strategic Command. Since then U.S Cyber Command has rapidly grown in size and scope of operations, with each military service establishing a cyber-component. By 2018, the command plans on having a Cyber Mission Force comprised of 133 teams organized into three types of teams. Each type will cover one of the DOD's three primary cyber missions: Cyber Protection Teams to defend DOD networks, systems, and information; Combat Mission Teams to support military operational and contingency plans; and National Mission Teams to defend the U.S. and its interests against cyber-attacks of significant consequence.[14]

As U.S. cyberspace operations have expanded, a very centralized philosophy of command and control has been adopted. The global, trans-regional nature of the domain allows for centralized command, control, planning, and execution of cyberspace operations.[15] This has created a conflict between U.S. Cyber Command and the combatant commanders (CCDRs) who see cyberspace as another operational domain in which they need to integrate their forces towards accomplishment of their objectives.[16] It is difficult for CCDRs to integrate cyberspace operations into their warfighting plans when many cyberspace operations are conducted by individuals sitting in Fort Meade, Maryland. Even though cyber support elements (CSE) can be

---

[14] U.S. Department of Defense, *The Department of Defense Cyber Strategy*, accessed 25 April 2015, http://www.defense.gov/home/features/2015/0415_cyber_strategy/.

[15] Chairman, U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication (JP) 3-12R (Washington, DC: CJCS, 5 February 2013), II-6.

[16] In relation to regional [sic] combatant commanders: Col. David C. Hathaway, *The Digital Kasserine Pass: The Battle Over Command and Control of DoD's Cyber Forces* (21st Century Defense Initiative Policy Paper, Foreign Policy at Brookings: Brookings Institute, 15 July 2011), Accessed 20 April, 2015. http://www.brookings.edu/~/media/research/files/papers/2011/7/15%20cyber% 20forces%20hathaway/ 0715_cyber_forces_hathaway.pdf, iv.
Functional Combatant Commanders, like U.S. Special Operations Command, may also have a conflict based on their desire to use cyberspace operations as part of their functional duties: U.S. Special Operations Command *United States Special Operations Command 2020 (SOCOM2020)*, accessed 30 April 2015, http://www.defenseinnovationmarketplace. mil/resources/SOCOM2020Strategy.pdf, 3.

located with geographic CCDRs for reach back to Ft. Meade, the CSEs remain under operational control[17] (OPCON) to U.S. Cyber Command.[18] The centralization of U.S. cyber command and control has left geographic CCDRs feeling like they do not have command of a cyber-capability like they do of other warfighting forces, but rather they must ask U.S. Cyber Command or higher for approval and execution of effects in cyberspace.[19]

## INNOVATION THROUGH DECENTRALIZATION AND DISAGGREGATION

Considering the rapid growth of U.S. Cyber Command, combined with the rapidly accelerating expansion of cyberspace, cyberspace operations should decentralize and disaggregate to capitalize on every opportunity for an innovative advantage. Centralized command and control does not take advantage of the innovation that can be gained from more people freely working on an issue. Pushing capability and authority as low as possible, even to the tactical level, will encourage cyber employment and innovation that will take advantage of the discovery of unanticipated applications.[20] Secretary of Defense Ashton Carter's April 2015 DoD Cyber Strategy acknowledges the worth of the men and women in the Cyber Mission Forces as being U.S. Cyber Command's source of strength and inspiration.[21] This fact is recognized by maneuver warfare's high level of trust in its decentralized command and control philosophy. By instilling trust at every level, service members feel free to innovate and explore

[17] Operational Control (OPCON): Command authority that may be exercised by commanders at any echelon below the level of combatant command to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command (JP 3-0, *Joint Operations*, 11 Aug 2011).
[18] Chairman, U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication (JP) 3-12R (Washington, DC: CJCS, 5 February 2013), III-6.
[19] Ben Fitzgerald and LtCol Parker Wright, *Digital Theaters: Decentralizing Cyber Command and Control* (Disruptive Defense Papers: Center for a New American Security, April 2014), accessed 20 April 2015, http://www.cnas.org/sites/default/files/publications-pdf/CNAS_DigitalTheaters_FitzGeraldWright.pdf, 15.
[20] Ibid, 15.
[21] U.S. Department of Defense, *The Department of Defense Cyber Strategy* (Washington, DC: SECDEF, 17 April 2015), 33.

new ideas. An innovative culture is the foundation of an organization that develops new ways of operating from the bottom up. The power of many brains working on any given problem, without being stifled by strict command and control, will allow for the development of numerous and unique solutions to problems.

A decentralized command and control organization will instill an innovative organizational culture. Innovation will be able to freely prosper in an environment where every idea does not have to be passed up a bureaucratic chain of command for approval by individuals far removed from the situation. U.S. cyber leadership must encourage free and open thought at every level and delegate decision making authority down to the lowest possible level to facilitate an innovative culture.

Leaders must also understand that innovation is not maximized in a top down organization where direction is passed down to executors that have little to no input to the process. In this case, a few individuals are deciding how the organization should proceed, while the execution of directed tasks is the only thing left up to the individuals. Top level leaders pass guidance and intent, then trust individuals to simply carry out their tasks. It becomes apparent that even the trust inherent to mission command does not allow for enough freedom of thought or action to promote innovation. The freedom provided to subordinates by maneuver warfare's decentralized command and control is a requirement for the organizational innovation needed to operate in a fluid and uncertain environment.[22] U.S. Cyber Command should embrace the most decentralized command and control structure to develop a culture of innovation that can remain operationally effective in the dynamic cyber domain.

[22] Dan Buchner and David Horth, *Innovation Leadership*, (Greensboro: Center for Creative Leadership, 2014), accessed 30 April 2015, https://www.ccl.org/leadership/pdf/ research/ innovationleadership.pdf, 15.

The exploitation of innovation by decentralizing command and control to lower levels will be greatly aided by further disaggregating U.S. cyberspace operations. Innovation can be increased when the cyber mission force is working in different environments where they will gain a wide range of perspectives. As Ben Fitzgerald and LtCol Parker Wright recognize in *Digital Theaters: Decentralizing Cyber Command and Control*, "Fielded units are more likely to develop and nurture tactical applications and to envision new ways of employing cyber at the tactical level. They know where cyber could be applied to replace or reinforce current service capabilities, and they have a better understanding of the systems and the processes unique to their service."[23] Disaggregating the force will put physical, as well as the needed organizational, distance between operators and the top of cyber leadership to maximize innovation.

Many military service members that work in cyberspace already work a great distance from U.S. Cyber Command. These individuals are spread across units providing local network security and other information technology assistance. But they lack a connection back to U.S. Cyber Command and are not as highly trained as the Cyber Mission Force operators. Therefore, the distant environments occupied by U.S. military forces should also be appropriately accounted for in the Cyber Mission Force's locations.

Each type of team within the Cyber Mission Force could decentralize and disaggregate so that they can best complete their cyber mission and still provide innovative feedback to the hub at U.S. Cyber Command. Cyber Protection Teams that defend DOD networks could gain a greater appreciation for the scope of their job by visiting and/or being stationed across the breadth of U.S. military global locations. By visiting distant locations, where local network

[23] Ben Fitzgerald and LtCol Parker Wright, *Digital Theaters: Decentralizing Cyber Command and Control* (Disruptive Defense Papers: Center for a New American Security, April 2014), accessed 20 April 2015, http://www.cnas.org/sites/default/files/publications-pdf/CNAS_DigitalTheaters_FitzGeraldWright.pdf, 15.

administrators operate daily, the Cyber Protection Teams will gain a greater understanding of network needs, threat capabilities, and local defense difficulties. Additional teams could be stationed at critical locations to better support the network defense of the other domains' warfighters. All teams would be able to share information to increase the overall security and defense of DODs networks.

Combat Mission Teams should be pushed forward from U.S. Cyber Command, like the Cyber Protection Teams, but they also need the greatest command distance to better support combatant commanders. They are tasked with generating integrated cyber effects for operational plans and contingency operations, and they can best do this by being collocated with their supported combatant command. U.S. Cyber Command must allow combatant and joint force commanders to exercise command and control, at a minimum of the OPCON level, of their assigned or supporting cyber forces. By working for and supporting the combatant or joint force commanders directly, the Combat Mission Teams will understand how to apply their unique skills towards accomplishment of their commanders' tasking. They will have a far better understanding of the operating environment of non-cyber forces and will be able to apply this perspective to their cyber support of operational objectives.

Compared to Combat Mission and Cyber Protection Teams, the National Mission Teams that defend the U.S. and its interests against cyber-attacks may need to remain more centralized. Their mission set is mainly based in the continental United States (CONUS). However, those teams may be able to better defend critical, cyberspace-reliant U.S. infrastructure by placing themselves in close proximity to their defended asset. For example, a National Mission Team could be placed at or near a nuclear power plant to understand how the asset works both inside and outside of cyberspace. The team could still have robust connectivity to U.S. Cyber

Command, but would develop a wider perspective of their duties than if they were physically sitting in the same building as the DOD cyber leadership. These wider perspectives will produce a set of lessons learned and best practices that can be applied to the defense of other critical U.S. assets.

Leaders at U.S. Cyber Command must decentralize and disaggregate the Cyber Mission Force to take advantage of the perspectives gained from varied operating environments. Only by operating in a dispersed and decentralized manner will each type of cyber team develop the best methods of supporting their assigned mission. Decentralization of command and control across the Cyber Mission Force will increase freedom of thought and action that will change the organizational culture. In addition, personal and organizational relationships will develop between cyber operators and those that they support, further contributing to effective military cyberspace operations. It will take operating in this way over time to develop the culture needed to innovatively operate in cyberspace. Short term decisions, even from smart, free thinking leaders, are not the answer. Only long term cultural changes will improve the process to develop innovative outputs that can keep U.S. cyberspace operations on the technological edge.[24]

## OBJECTIVE ACCOMPLISHMENT THROUGH DECENTRALIZATION

Just as it can best maximize innovation, decentralization of cyber command and control will best contribute to the accomplishment of military objectives. Military objectives should be the focus of operations in every domain, with command and control as the driving force. Decentralizing cyberspace operations will allow the proper focus on military objectives.

[24] Williamson Murray, "Innovation: Past and Future," *Joint Force Quarterly*, Summer 1996, 52.

Cyberspace operations cannot be limited to strategic applications, but must be made available to operational and tactical levels through the geographic CCDRs.[25]

Geographic CCDRs develop plans to execute operations in their area of responsibility (AOR). They accomplish series of objectives that in turn contribute to higher strategies or policies. To this end, they should command and control forces in every warfighting domain within their AOR. Unity of command is defined as the commander having the requisite authority to direct and employ his forces in pursuit of a common objective.[26] Geographic CCDRs must have unity of command to ensure unity of effort towards objective accomplishment.[27]

Decentralization of cyberspace operations away from U.S. Cyber Command to the geographic CCDRs is the only way to ensure both unity of command and effort towards objectives in their AOR. To do otherwise would be to deny geographic CCDRs the warfighting capability in one of the five domains. Centralized command and control of cyberspace operations at U.S. Cyber Command is a vulnerability for geographic CCDRs. This vulnerability can be exploited by adversaries who will combat U.S. forces with every warfighting capability at hand. This self-induced weakness can be mitigated by greater decentralization of command and control as called for by maneuver warfare doctrine.

Geographic CCDRs should have command and control of cyber forces and authority to execute cyberspace operations as long as the effects remain in their AOR or are coordinated with another combatant commander. Facilitation of fires and effects is accomplished in other

[25] Ben Fitzgerald and LtCol Parker Wright, *Digital Theaters: Decentralizing Cyber Command and Control* (Disruptive Defense Papers: Center for a New American Security, April 2014), accessed 20 April 2015, http://www.cnas.org/sites/default/files/publications-pdf/CNAS_DigitalTheaters_FitzGeraldWright.pdf, 14.
[26] Chairman, U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication (JP) 3-0 (Washington DC: CJCS, 11 August 2011), GL-18.
[27] Ibid, A-2.

domains by using fire support coordination measures (FSCM).[28] Cyber FSCMs should be developed to coordinate and integrate cyberspace operations between command organizations instead of accepting the weakness inherent to centralized command and control.

Even joint cyber doctrine, JP 3-12R *Cyberspace Operations,* tell us that "commanders integrate cyberspace capabilities at all levels and in all military operations,"[29] However, CCDRs feel that U.S. Cyber Command doles out cyber capability instead of allowing CCDRs to have a guaranteed cyber capability for integration into every level of their plans and operations.[30] Therefore, U.S. Cyber Command should follow their own doctrine to allow cyber integration at every level by adopting maneuver warfare's decentralized command and control.

Giving geographic CCDRs full combatant command authority[31] over cyber forces would provide the greatest amount of flexibility in using those forces for objective accomplishment. At the very least, geographic CCDRs should have OPCON of cyber forces to fully integrate them as required. A simple tactical control[32] of, or supporting role by, cyber forces will not provide geographic CCDRs sufficient unity of command for effectiveness in a fluid warfighting environment. With higher levels of command authority, geographic CCDRs can organize cyber forces or further delegate command and control to best support national strategies and policies.

---

[28] Chairman, U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication (JP) 3-12R (Washington, DC: CJCS, 5 February 2013), IV-9.
[29]Ibid, IV-1.
[30] Ben Fitzgerald and LtCol Parker Wright, *Digital Theaters: Decentralizing Cyber Command and Control* (Disruptive Defense Papers: Center for a New American Security, April 2014), accessed 20 April 2015, http://www.cnas.org/sites/default/files/publications-pdf/CNAS_DigitalTheaters_FitzGeraldWright.pdf, 15.
[31] Combatant Command (COCOM): The authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command (JP 3-0, *Joint Operations*, 11 Aug 2011).
[32] Tactical Control (TACON): Command authority over assigned forces or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned (JP 3-0, *Joint Operations*, 11 Aug 2011).

CCDRs can achieve cross-domain synergy and dominance in modern conflict if DOD leadership arms them appropriately by giving them command and control of cyber forces.

Commanders accomplish objectives during conflict by breaking them down into sub-objectives and assigning those sub-objectives to the proper command level. This allows the appropriate focus by each level of the chain of command. Decentralizing down to the tactical level is needed if cyberspace operations are to become a viable and reliable military option.[33] Centralized cyber command and control does not delegate sub-objectives or tasks, much less allow for tactical cyberspace operations.

In maneuver warfare, the senior commander delegates authority and prescribes lower level commanders' actions only to the degree that is essential for coordination.[34] So long as actions are coordinated with adjacent forces, maneuver warfare encourages initiative at every level. As stated in Marine Corps Doctrinal Publication 1, *Warfighting*: "It is this freedom for initiative that permits the high tempo of operations that we desire. Uninhibited by excessive restrictions from above, subordinates can adapt their actions to the changing situation. They inform the commander of what they have done, but they do not wait for permission".[35] High levels of initiative are possible when subordinates understand their commander's intent. Each mission is comprised of two parts: the task to be accomplished and the reason or intent behind

[33] Ben Fitzgerald and LtCol Parker Wright, *Digital Theaters: Decentralizing Cyber Command and Control* (Disruptive Defense Papers: Center for a New American Security, April 2014), accessed 20 April 2015, http://www.cnas.org/sites/default/files/publications-pdf/CNAS_DigitalTheaters_FitzGeraldWright.pdf, 15.
[34] U.S. Marine Corps, *Warfighting*, Marine Corps Doctrinal Publication (MCDP) 1 (Washington, DC: Headquarters U.S. Marine Corps, 1997), 87.
[35] Ibid, 88.

it.[36] The commander's intent explains the "why?" behind a mission, and allows subordinates to, "grasp how their actions fit into the larger situation."[37]

With proper commander's intent, U.S. cyberspace operations can use maneuver warfare's high degree of initiative to better accomplish objectives. By understanding higher headquarters' intent, lower level commanders can accomplish sub-objectives through cyber actions without overstepping their authorities or creating unnecessary collateral damage. Many lower commanders working in a decentralized command and control construct will each focus precisely on their tasks. This task sharing creates a greater cumulative synergy towards larger objective accomplishment than can be carried out by a few centralized commanders. Centralizing command and control at U.S. Cyber Command cannot accomplish military objectives as well as if each level of the chain of command integrates cyberspace operations towards their sub-objectives.

The full potential of cyber capabilities towards objective accomplishment can only be realized by being institutionalized alongside other theater warfighting functions. Beginning with operational planning, cyber capabilities must be fully integrated at the combatant commander level and below. The required level of details needed by CCDRs and below during planning cannot be accomplished with dislocated, centralized cyber forces.

Before planning shifts into execution, commanders must already have been delegated cyber command authority to dynamically direct all forces as the joint battlespace evolves. This evolution can happen at the speed of light in cyberspace. Commanders must be able to

---

[36] Paraphrase of the mission definition from Chairman, U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication (JP) 3-0 (Washington DC: CJCS, 11 August 2011), GL-13. As found in U.S. Marine Corps, *Warfighting*, Marine Corps Doctrinal Publication (MCDP) 1 (Washington, DC: Headquarters U.S. Marine Corps, 1997), 89.

[37] U.S. Marine Corps, *Warfighting*, Marine Corps Doctrinal Publication (MCDP) 1 (Washington, DC: Headquarters U.S. Marine Corps, 1997), 88.

command and control at a similar speed, vice being hampered by a cumbersome command structure or multiple chains of command.

By focusing the cyber command and control discussion on the accomplishment of operational objectives, it becomes clear that maneuver warfare's decentralized command and control should be adopted. Its flexible and adaptive structure allows for cyber forces and command authorities to be placed where they will be most effective to attain geographic CCDRs' goals. These geographic CCDRs are best placed to integrate forces from each warfighting domain to accomplish the military objectives that will support national strategies and policies.

## CYBERSPACE OPERATIONS IN AN A2AD ENVIRONMENT

Decentralized cyberspace command and control is needed by CCDRs to accomplish joint military objectives in a major theater anti-access, area denial (A2AD) environment. The near total reliance on cyberspace is a major weakness of centralized command and control because it relies on communications paths to pass commanders' direction to the warfighters.[38] Without those paths commanders will lose their ability to command and control.

Command, control, and communications architecture will likely be an initial target and early casualty of A2AD warfare. Military leaders understand that an entire campaign can be undermined by an attack on DOD networks that compromises U.S. force's command and control systems.[39] The reliance on high tech communication paths and cyberspace has two large vulnerabilities. Both the availability of electricity and the requirement for network connectivity make centralized command and control very vulnerable to an A2AD-capable adversary.

---

[38] Richard M. Crowell, *War in the Information Age: A Primer for Information Operations and Cyberspace Operations in 21st Century Warfare (NWC 2021C)* (U.S. Naval War College, Joint Military Operations Department, Newport, RI: U.S Naval War College, January 2015), 38.

[39] Col. David C. Hathaway, *The Digital Kasserine Pass: The Battle Over Command and Control of DoD's Cyber Forces* (21st Century Defense Initiative Policy Paper, Foreign Policy at Brookings: Brookings Institute, 15 July 2011), Accessed 20 April, 2015. http://www.brookings.edu/~/media/research/files/papers/2011/7/15%20cyber%20forces%20hathaway/0715_cyber_forces_hathaway.pdf, 2.

Decentralizing command and control is the most effective way to minimize vulnerabilities and maximize cyberspace operations in an A2AD conflict.

A2AD conflict will have much greater tempo than any military operations possibly since the 2003 invasion of Iraq. Maneuver warfare doctrine exploits the natural disorder of high tempo military operations.[40] This is only possible with a widely decentralized command and control philosophy that not only allows forces to fight in the face of disorder, but seeks to generate disorder and use it as a weapon against an adversary.[41] U.S. cyberspace operations should not only seek to thrive in the disorderly environment caused by an A2AD adversary, but they should create equal or greater disorder and uncertainty for the adversary.

To date, U.S. cyber forces have not fought in the uncertainty of a large scale A2AD environment. The resulting evolution of command and control, centered on U.S. Cyber Command and higher levels of national leadership, is a byproduct of low-intensity, steady-state operations.[42] This higher headquarters focused command and control structure will simply be overwhelmed in the complex and rapidly changing environment of a full scale, A2AD war.

A2AD warfare will degrade connectivity and bandwidth, while a centralized architecture requires bandwidth to both execute cyberspace operations and complete command and control responsibilities. More decentralization will alleviate a portion of the reach back requirements of the current structure. Once again, joint cyber doctrine should be followed by U.S. Cyber

[40] U.S. Marine Corps, *Warfighting*, Marine Corps Doctrinal Publication (MCDP) 1 (Washington, DC: Headquarters U.S. Marine Corps, 1997), 11.
[41] Ibid, 12.
[42] Richard M. Crowell, *War in the Information Age: A Primer for Information Operations and Cyberspace Operations in 21st Century Warfare (NWC 2021C)* (U.S. Naval War College, Joint Military Operations Department, Newport, RI: U.S Naval War College, January 2015), 40.

Command to allow operations under degraded cyberspace conditions by adopting maneuver warfare's decentralized command and control philosophy.[43]

Whereas centrally executed cyberspace operations from CONUS will likely lose or have degraded connectivity to the theater of A2AD conflict, decentralized and disaggregated theater cyber forces may still have operational capability. Local connectivity may be possible even though connectivity to U.S. Cyber Command is lost. These forces will only be able to operate effectively to support military objectives if cyber command and control is decentralized. In some cases, theater cyber forces may have the ability to execute cyber effects against an adversary that helps U.S. Cyber Command regain global connectivity.

Global connectivity may be incorrectly assumed when considering the global nature of cyberspace as a warfighting domain.[44] Cyberspace is a global domain of interconnected networks, inside of which cyberspace operations can still take place with or without connectivity on a global scale. A decentralized command and control structure would allow U.S. Cyber Command to operate in the worst case of a degraded and disconnected cyber environment.

Operating in a decentralized manner that accounts for the degraded nature of an A2AD environment must immediately be undertaken by U.S. Cyber Command. Otherwise, cyberspace operations will falter just when needed most if cyber forces wait until A2AD warfare erupts to decentralized command and control doctrine and philosophy. That change must happen now, before conflict escalation. Cyber forces should be organized for warfighting and then adapted as needed for peacetime, rather than vice versa.[45] Organization and training for A2AD warfare, and

[43] Chairman, U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication (JP) 3-12R (Washington, DC: CJCS, 5 February 2013), I-1.
[44]Ibid, I-2.
[45] U.S. Marine Corps, *Warfighting*, Marine Corps Doctrinal Publication (MCDP) 1 (Washington, DC: Headquarters U.S. Marine Corps, 1997), 55.

thereby being prepared for it, begins with U.S. cyber forces adopting and embracing maneuver warfare's decentralized command and control at the structural, doctrinal, and philosophical level.

## COUNTER ARGUMENT

Due to the unforeseen, unknown consequences of military cyberspace operations, and the sensitivities associated with them, cyber command and control must remain tightly centralized. Additionally, the technological advances of cyberspace allow for corresponding centralization of execution. The high demand, low density nature of cyber forces, as well as their legal and political considerations, lend themselves to centralization as the best structure for U.S. military cyberspace operations.[46]

Only through centralized operations can U.S. cyber forces understand and account for the global possibilities of cyber effects.[47] If cyber forces were spread amongst the CCDRs, they would inevitably fail to foresee the cross-AOR or cross-functional global effects of their cyber actions. A well-meaning, but uninformed combatant commander lacks the technical knowledge and global perspective needed to utilize assigned cyber forces as intended, designed, and to the fullest extent possible.[48] Much like strategic aviation operations, cyberspace operations must be controlled by a single or few individuals who maintain "the broad, strategic perspective necessary to balance and prioritize the use of a powerful, highly desired yet limited force."[49]

However, the human dimension of war will not be diminished by technology, the risk of uncertainty will never be eliminated, and global situational awareness is an unachievable

---

[46] Chairman, U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication (JP) 3-12R (Washington, DC: CJCS, 5 February 2013), I-7.
[47] Ibid, I-7.
[48] Ben Fitzgerald and LtCol Parker Wright, *Digital Theaters: Decentralizing Cyber Command and Control* (Disruptive Defense Papers: Center for a New American Security, April 2014), accessed 20 April 2015, http://www.cnas.org/sites/default/files/publications-pdf/CNAS_DigitalTheaters_FitzGeraldWright.pdf, 13.
[49] U.S. Air Force, *Air Force Basic Doctrine, Organization, and Command*, Air Force Doctrinal Document (AFDD) 1 (Washington, DC: Secretary of the Air Force, 14 October, 2011), 38.

fallacy.[50] The U.S. military already operates at all levels in cyberspace to accomplish day-to-day activities. Subsequently, commanders and operators have a higher understanding of the range of operational effects that could result from a given cyberspace operation than may be assumed in current cyberspace policies. These commanders and operators can be relied upon to execute decentralized command and control of cyberspace operations, while remaining within the commander's intent.

## CONCLUSION

Maneuver warfare doctrine tells us that, "efforts to fully centralize military operations and exert complete control by a single decision maker are inconsistent with the intrinsically complex and distributed nature of war."[51] This is an accurate acknowledgment of the nature of war and conflict, regardless of the operating domain. Cyberspace may be the most complex and distributed of the warfighting domains due to its rapid expandability, technological inertia, and relative infancy as a military operating environment, however it has not changed the nature of war. Risk from uncertainty cannot be reduced to zero in cyberspace any more than in the physical domains. With maneuver warfare doctrine, and its decentralized command and control, cyber warfighters can operate effectively despite uncertainty through simple, flexible plans and by fostering initiative among subordinates.[52]

Cyberspace operations in this fluid domain cannot rely on a rigid, centralized command and control system. To operate effectively in the highly dynamic cyber domain, the U.S. military must conduct cyberspace operations with an equally nimble command and control system. It must take advantage of the flexibility and high tempo that maneuver warfare's

[50] U.S. Marine Corps, *Warfighting*, Marine Corps Doctrinal Publication (MCDP) 1 (Washington, DC: Headquarters U.S. Marine Corps, 1997), 14.
[51] Ibid, 13.
[52] Ibid, 8.

decentralized command and control provides. Decisions should be pushed to the lowest level to avoid losing time when lower echelons possess the skill and judgment to act within commander's intent.

By decentralizing command and control, U.S Cyber Command can increase the organizational innovation as a whole by capitalizing on the power of the collective individuals. By delegating command and control to the lowest level possible, by clearly articulating commander's intent, and by trusting individuals to make decisions and take appropriate action, U.S. cyberspace operations will be most effective in accomplishing military objectives while remaining cognizant of the risks of unintended cyber effects. These actions are necessary for the U.S. to remain dominate in all warfighting domains despite advanced adversaries and threat environments. Had special operations team 2835 been trusted to operate in this manner, they would have executed a tactical cyberspace operation, in accordance with commander's intent, with positive operational and strategic effects towards greater U.S. national security.

## RECOMMENDATIONS

1) DOD and U.S. Strategic Command should conduct a review to determine if U.S. Cyber Command should remain as a sub-unified command within U.S. Strategic Command or become a functional combatant command.
2) U.S. Cyber Command should conduct a review of command and control doctrine to ensure maximum flexibility and preparedness for the future threat environment by all Cyber Mission Forces. Adopted changes should take into account the needs and responsibilities of geographic and functional combatant commanders. The widest possible decentralization and delegation of cyber forces and command authorities should be undertaken.
3) U.S. Cyber Command should implement changes across the board through organizational structure, training exercises, steady-state operations, and operational plans. The new command and control doctrine must be embraced from the highest levels of the chain of command, through combatant commanders, and down to the tactical cyberspace operators.

## SELECTED BIBLIOGRAPHY


Basla, Michael J. *The Cyber Domain: How is it Changing the Warfighter*. RUSI Defence Systems Vol. 12, No. 1, June 2009. pp: 67- 70. London, England, 2009. Accessed 13 Mar 2015. https://www.rusi.org/downloads/assets/Cyber_Domain_and_the_Warfighter_ RDS_Summer_09.pdf.

Buchner, Dan and David Horth. *Innovation Leadership*. White Paper. Greensboro: Center for Creative Leadership, 2014. Accessed 30 April 2015. https://www.ccl.org/leadership/pdf/ research/ innovationleadership.pdf.

Crowell, Richard M. *Some Principles of Cyber Warfare (NWC 2160)*. U.S. Naval War College, Joint Military Operations Department, Newport, RI: U.S. Naval War College, January 2015.

———. *War in the Information Age: A Primer for Information Operations and Cyberspace Operations in 21st Century Warfare (NWC 2021C)*. U.S. Naval War College, Joint Military Operations Department, Newport, RI: U.S Naval War College, January 2015.

Fitzgerald, Ben and LtCol Parker Wright. *Digital Theaters: Decentralizing Cyber Command and Control*. Disruptive Defense Papers: Center for a New American Security, April 2014. Accessed 20 April 2015. http://www.cnas.org/sites/default/files/publications-pdf/ CNAS_ DigitalTheaters_FitzGeraldWright.pdf.

Fryer-Biggs, Zachary. *Panetta Green Lights First Cyber Operations Plan*. Defense News, 6 June 2012. Accessed 13 April 2015. http://archive.defensenews.com/article/ 20120606/ DEFREG02/306060010/Panetta-Green-Lights-First-Cyber-Operations-Plan.

Gates, Robert M. U.S. Secretary of Defense. *Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations*. Memorandum for the Secretaries of the Military Departments, et al. Washington DC: SECDEF, 23 June 2009.

Gould, Joe. *Former NSA Chief: Follow SOCOM Model for Cyber*. Defense News, 17 April 2015. Accessed 20 April 2015. http://www.defensenews.com/stroy/defense-news/blog/intercepts/2014/04/17/keith-alexander-cyber-dod-aei/25951903/.

Hathaway, Col. David C. *The Digital Kasserine Pass: The Battle Over Command and Control of DoD's Cyber Forces*. 21st Century Defense Initiative Policy Paper. Foreign Policy at Brookings: Brookings Institute, 15 July 2011. Accessed 20 April, 2015. http://www.brookings.edu/~/media/research/files/papers/2011/7/15%20cyber%20forces %20hathaway/0715_cyber_forces_hathaway.pdf

Hughes, Rex. *A Treaty for Cyberspace*. International Affairs 86: 2, March 2010. pp 523-544. Accessed 20 April, 2015. http://www.cyberdialogue.ca/wp-content/uploads/2011/03/Rex-Hughes-A-Treaty-for-Cyberspace.pdf.

Libicki, Martin C. *Cyberspace is Not a War-Fighting Domain*. I/S: A Journal of Law and Diplomacy for the Information Society, Vol. 8, Issue 2, 2012, pp: 321-336. Columbus, OH, 2012. Accessed 13 March 2015. http://moritzlaw.osu.edu/students/ groups/is/ files/2012/02/4.Libicki.pdf.

Liddell Hart, B.H. *The Objective in War, National object and Military Aim*, Lecture at Naval War College 24 Sep 1952, published in Naval War College Review Vol. V No. 4, pp: 1-30, Dec 1952, unclassified 15 Dec 1953 Ref: ALNav 59-53 (NWC 2044)

Lind, William S. *Maneuver Warfare Handbook*. Boulder: Westview Press, 1985.

*Moore's Law or How Overall Processing Power for Computers will Double Every Two Years*. Accessed 21 April 2015. http://www.mooreslaw.org/.

Murray, Williamson." Innovation: Past and Future," *Joint Force Quarterly*, Summer 1996, 51-60.

Oliver, Irvin. *Cyber Operations in Strategic Landpower: Army Cyber Operations and War Fighting Functions in Strategic Landpower*. Accessed 13 March 2015, http://www.tradoc.army.mil/stlp/docs/pubs/140220%20CYBER%20IN%20STRATEGIC%20LANDPOWER.pdf.

U.S. Air Force. *Air Force Basic Doctrine, Organization, and Command*. Air Force Doctrinal Document (AFDD) 1. Washington, DC: Secretary of the Air Force, 14 October, 2011.

U.S. Department of Defense. *The Cyber Domain Security and Operations*. Accessed 13 April 2015. http://www.defense.gov/home/features/2013/0713_cyberdomain/.

———. *The Department of Defense Cyber Strategy*. Accessed 25 April 2015. http://www.defense.gov/home/features/2015/0415_cyber_strategy/.

———. *The Department of Defense Cyber Strategy*. Washington, DC: SECDEF, 17 April 2015.

U.S. Marine Corps. *Warfighting*. Marine Corps Doctrinal Publication (MCDP) 1. Washington, DC: Headquarters U.S. Marine Corps, 1997.

———. *Command and Control*. Marine Corps Doctrinal Publication (MCDP) 6. Washington, DC: Headquarters U.S. Marine Corps, 1996.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Cyberspace Operations*. Joint Publication (JP) 3-12R. Washington, DC: CJCS, 5 February 2013.

———. *Desired Leader Attributes for Joint Force 2020*. CJCS Memorandum, CM-0166-13, 28 June 2013. (NWC 1194).

———. *Joint Operations*. Joint Publication (JP) 3-0. Washington DC: CJCS, 11 August 2011.

———. *Mission Command*. White Paper. Washington, DC: CJCS, 3 April 2012.

U.S. Special Operations Command. *United States Special Operations Command 2020 (SOCOM 2020)*. Accessed 30 April 2015. http://www.defenseinnovationmarketplace.mil/resources/SOCOM2020Strategy.pdf.