REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
20-04-2016	Master's of Military Studies	SEP 2015 - APR 2016

4. TITLE AND SUBTITLE
Institutionalizing Cyberspace into the Joint Task Force

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Smith, Kevin, A, Major, USMC

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
Matthew J. Flynn, Ph.D.

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Cyberspace is a domain created by people and the concept of C2 is important in cyberspace. There is the need to link cyber strategy identified in policy with tactics via doctrine that speaks to cyberspace operations at the operational level. That operational level exists in the campaigns conducted primarily by the JTFs comprised of components from each branch of service. Each branch of service has service-specific information technology and C2 capabilities, and they are required to be interoperable. To gain better C2 of the cyber battlespace, a JTF needs doctrine applicable to cyber C2 systems, cyber situational awareness, command authorities for cyber, and cyber support to the warfighting functions. Once this is achieved the service components supporting the JTF can provide synergistic cyber capabilities to the JTF. Referencing existing doctrine will help in the development of effective doctrine for cyberspace. The cyber domain represents the ultimate C2 system. Current doctrine is inadequate in describing how C2 of the cyber domain is attained. Unique command relationships and command authorities are of particular importance to cyber C2. With cyberspace as a warfighting domain, the JTF needs to employ cyber capabilities in support of all joint warfighting functions.

15. SUBJECT TERMS
Command and Control; Cyber Doctrine; Command and Control Doctrine; Command and Control Systems

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
Unclass	Unclass	Unclass	UU	38	19b. TELEPHONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

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

MASTER OF MILITARY STUDIES

TITLE:

Institutionalizing Cyberspace into the Joint Task Force

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

AUTHOR:
Kevin A. Smith
Major USMC

AY 15-16

Mentor and Oral Defense Committee Member: _____
Approved: _____
Date: _____

Oral Defense Committee Member: _____
Approved: _____
Date: _____

Executive Summary

Title: Institutionalizing Cyberspace into the Joint Task Force

Author: Major Kevin A. Smith, United States Marine Corps

Thesis: Service-specific cyber capabilities need to be interoperable and able to support how the United States conducts military operations in the joint environment. This reinforces the need for effective doctrine for command and control (C2) of the Joint Task Force (JTF) cyber battlespace to be effective in terms of utilizing cyber power in military operations.

Discussion: Cyberspace exists as a domain created by people, and the concept of C2 is the most important function in cyberspace. There is the need to link cyber strategy identified in policy with tactics via doctrine that speaks to planning and executing cyberspace operations at the operational level. That operational level exists in the campaigns conducted primarily by the JTFs comprised of components from each branch of service. Each branch of service has service-specific information technology and C2 capabilities, and they are required to be interoperable. In order to gain better C2 of the cyber battlespace, a JTF needs doctrine applicable to cyber C2 systems, cyber situational awareness, command authorities for cyber, and cyber support to the warfighting functions through offensive cyber operations, defensive cyber operations, and DODIN operations. Once this is achieved the service components supporting the JTF can provide synergistic cyber capabilities to the JTF. Referencing existing doctrine that is not specific to cyberspace will help in the development of effective new doctrine for cyberspace.

Conclusion: The cyber domain represents the ultimate C2 system. The current cyber doctrine is inadequate in describing how C2 of the cyber domain is attained. Unique command relationships and command authorities are of particular importance to cyber C2. With the consideration of cyberspace as a warfighting domain, the JTF needs to employ cyber capabilities in support of all joint warfighting functions.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Illustrations

Page

Table of Contents

Preface

Issues regarding military cyberspace operations and the cyber warfighting domain can be highly complex and abstract in comparison to traditional military studies. Technology has consistently played a significant role in the evolution of warfighting, and this technological influence is most astonishing with the recent emergence of the cyber warfighting domain. Within this emerging discipline of military cyber operations there has been great interest in the discussion of its characteristics and how cyber warfare will unfold on the future battlefield. Due to the relative infancy of the cyber warfighting domain there are numerous opportunities for research and discussion. Overdependence on cyberspace will make us vulnerable. At the same time, increasing our operations and capabilities in cyberspace has the potential for achieving the greatest efficiency ever.

This research is intended to address one of the areas of cyberspace that can currently be confusing. It approaches the topic of command and control of cyberspace at the operational level as the link to institutionalize cyberspace concepts within U.S. military operations. The resulting topic of this paper is that the current doctrine is inadequate. Accurate and flexible joint doctrine is required for the future conduct of Joint Task Force operations, and for the service components to develop interoperable capabilities.

The guidance from Dr. Matthew J. Flynn was essential to this research. His mentorship and assistance was invaluable to this process. The efforts of the many individuals currently developing cyber capabilities and concepts in the Department of Defense are noteworthy, and the contribution they provide to the discussion is greatly appreciated. In particular, LtCol Gregory Wynn’s insights and assistance in attaining references were critical to this research.

Introduction

Joint Publication 3-12R defines cyberspace as "the global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Further, this doctrine defines cyberspace operations as the combination of defensive cyber operations (DCO), offensive cyber operations OCO, and Department of Defense Information Network (DODIN) capabilities to achieve objectives.[1]

The unique aspect that distinguishes cyberspace among other domains is the fact that it is manmade. Information technology, the Internet, telecommunications, and computers are all human creations. The fact that there is no physical characteristic that distinguishes it as in the physical ground, maritime, and air domains has led some to question whether it is a domain; but the modern capabilities in cyberspace are so extensive that it has become a domain in which the warfighter has to operate. Since cyberspace exists as a domain created by people, the human element must play a key role. In this respect, the concept of command and control is the most important function in cyberspace.

The current U.S. military doctrine that exists on cyberspace resides mainly at the strategic and tactical level, and it is inadequate. It does not clearly address how command and control of cyberspace will be achieved at the operational level. There is preexisting doctrine on command and control and joint operations, but it is not effective for operations in cyberspace. There is the need to link the strategy identified in policy with tactics via doctrine that speaks to planning and executing cyberspace operations at the operational level. That operational level exists in the campaigns conducted primarily by the Joint Task Forces.

Some within the military and cyberspace profession have suggested we may need a new branch of service for the Department of Defense's cyber capabilities, as Admiral James

Stavridis, U.S. Navy (Retired) and David Weinstein suggest in "Time for a U.S. Cyber Force."[2] Secretary of Defense Ash Carter stated at a visit to U.S. Cyber Command in March 2015 that he believes a separate branch of service may make sense in the future.[3] Some branches of service have created concepts for the cyber capabilities within their branch of service. Each service has service-specific information technology and command and control capabilities, and they are required to be interoperable. This consideration indicates a separate "cyber" branch of service would be a bad idea.

Service-specific cyber capabilities need to be interoperable and able to support how the United States conducts military operations in the joint environment. This reinforces the need for effective doctrine for command and control of the Joint Task Force cyber battlespace to be effective in terms of utilizing cyber power in military operations.

Others have identified the importance of doctrine and the need for doctrinal changes in the past. "Defining maneuver warfare for the Marine Corps," "The 'Maneuver Warfare' Concept," and "The Changing Face of War: Into the Fourth Generation" represent a series of articles published in the *Marine Corps Gazette* which sparked the professional debate about the concept of maneuver warfare and the changes to doctrine that would be required to educate and develop the forces on the concept. As Maj McKenzie noted, this debate led to the publication of *FMFM 1, Warfighting*, finally signaling the institutional acceptance of doctrine on maneuver warfare concepts of "how to fight."[4]

In order to gain better command and control (C2) of the cyber battlespace, a Joint Task Force (JTF) and the service components that provide them forces and equipment need doctrine applicable to cyber C2 systems, cyber situational awareness, command authorities for cyber, and cyber support to the warfighting functions. Once this is achieved the service components supporting the JTF can provide a total cyber capability that is greater than the sum of the individual service capabilities and the Joint Task Force will have freedom of movement in

cyberspace, and "cyber superiority" as defined by Lt Col Bonner.[5] With the resulting command and control of cyberspace, the commander will be able to visualize all domains and ensure appropriate actions are taking place. In this way, the U.S. military can better wage the cyber war.

Sources Review

Many within DoD have identified the fact that the concept of cyberspace, the cyber domain, and cyber operations are not new. A text in 1995 from the Joint Command and Control Warfare Staff Officer Course highlights many of the same aspects of cyber operations, and its historical connection to warfare:

> The idea of Command and Control Warfare (C2W) is as old as warfare itself. Destroying the adversary's capability to effectively command and control his forces is, always has been a lucrative military target. Additionally, protecting your own C2 has historically proven to be just as important to successful military operations. The idea has been around for a long time, but the strategy/tactics or the way we apply C2W is new.[6]
> (Armed Forces Staff College)

Electronic warfare used to attack the adversary's C2 and defend your own C2 is the main concept of C2W, and it is basically the same as today's cyberspace operations with a few exceptions. C2W is only a supporting effort of direct action through kinetic operations. This thinking about electronic warfare and the defense of C2 is a predecessor of cyberspace operations conceived prior to the extensive interconnectedness of today's military when the cyber domain had yet to be realized as a domain.[7]

The Deputy Secretary of Defense, William J. Lynn III, published the article "Defending a New Domain" in Sep/Oct 2010. In this article he presents cyberspace as an operational domain. The article describes the extensive cyber threats presented to the U.S. and the efforts to create the new organization of Cyber Command and is thus mainly strategic. However, several assumptions are presented about the general character of cyberspace. He describes cyberspace as a place for asymmetric warfare where weaker adversaries have a low "buy-in" to conduct operations against a stronger military. Offensive operations have the advantage as "the U.S.

government's ability to defend its networks always lags behind its adversaries' ability to exploit U.S. networks' weaknesses. Adept programmers will find vulnerabilities and overcome security measures put in place to prevent intrusions."[8] He also indicates that attribution is very difficult and this will impact the ability to deter.[9]

Jon Lindsay presents a compelling counter argument to Lynn's assumptions on cyberspace in his article, "Stuxnet and the Limits of Cyber Warfare." He uses the Stuxnet computer virus as an example of an offensive cyber attack conducted by an advanced military against a weaker force. The response to patch Stuxnet also shows that the global software security community is effective at providing timely defensive measures in cyberspace that minimize the desired offensive effect, and make the offensive cyber weapon irrelevant for future use by mitigating the software vulnerability it exploited.[10] The salient theme in Lynn and Lindsay's argument is that network defense, vulnerabilities, complex offensive actions, and attribution are key to the command and control of cyberspace.

In "Airpower, Spacepowers, and Cyberpower," Benjamin Lambeth presents the case that the principle of cyberspace as a warfighting domain is not new. He indicates that with modern technological advances, it has become the center of gravity for our nation's way of life. The new aspect it presents as a military domain is that "the classic constraints of distance, space, time and investment are reduced, in some cases dramatically, both for ourselves and for potential enemies."[11] Therefore, and similarly, operating in a new domain is not new and cyberspace need not push one back to having to rediscover new ideas and principles for acquisition there.

With the recent drive by the Department of Defense to build capability in the domain of cyberspace there emerges uncharted territory in law, policy, and doctrine. Commander Todd Huntley has contributed to the applicability of cyberspace to the Law of Armed Conflict in "Controlling the Use of Force in Cyber Space." His work has several implications for doctrine. "Overbroad use of the terms 'cyber attack' and 'cyber warfare' and a failure to clearly define the

various cyber capabilities also creates problems for the development of policy and doctrine for the use of these capabilities."[12] A doctrine that can effectively describe cyber capabilities, and account for the fact that cyber capabilities are frequently changing will be most effective for the Joint Forces Commander to employ them legally.[13] Likewise, a greater level of C2 will be attained within cyberspace.

Lincoln Bonner presents a concept of cyber superiority and cyber supremacy as analogous to aerial superiority and aerial interdiction in "Cyber Power in the 21st-Century Joint Warfare." He suggests that this is best employed in joint warfare by supporting "kinetic operations with a focus on supporting the air campaign."[14] The statement is accurate in practice considering the preferred modern way of war, but the cyber domain overlaps all the physical domains so the Joint Forces Commander should best employ cyber superiority and interdiction through command and control of the entire (all domains) campaign. Here is a refreshing look at C2 and cyberspace. Bonner is one of the few voices to directly address C2, his concept of cyber superiority already mentioned in this paper, and one that is key in terms of integrating cyber power into joint warfare.[15]

Inadequate Cyber Doctrine and the Use of Other Doctrine

Current doctrine on cyberspace inadequately supports joint forces and the Joint Task Force. The Goldwater-Nichols Department of Defense Reorganization Act of 1986 requires the U.S. to conduct military operations as a joint force. Each military branch of service provides forces as service components to the joint forces, normally operating as a Joint Task Force, consisting of a highly capable joint team representing capabilities of each service.[16] The U.S. employs the military through joint forces, and it is thus through the joint forces that cyber capabilities will be employed in support of U.S. military operations. The Joint Task Force Commander needs to be supported by interoperable service components and these joint forces need doctrine on cyberspace for the operational level that links the strategies and policies of

cyberspace with actions the Joint Task Force is taking in cyberspace. There are Joint Publications on Command and Control for Joint Air, Land, and Maritime Operations (JP 3-30, 31, & 32) but there is no solid doctrine specifically regarding the Command and Control of Joint Cyber Operations.

Joint Publication 3-12(R) Cyberspace Operations is the primary source of doctrine for the combatant commanders and their JTFs in conducting cyberspace operations. It is a relatively thorough tactical document that is of utility for defining and achieving a common understanding of some effective terms within cyberspace and cyber operations. The portion of the publication regarding command and control within cyberspace is totally insufficient. Its main contribution is a brief description of the command relationships for cyberspace operations based off the Transitional Cyberspace Operations Command and Control CONOPS; which has been modified since the publication of JP 3-12(R).[17] Exactly what is command and control of cyberspace needs to be defined. Cyberspace is a different domain with a unique C2 System, concepts of situational awareness, and unique functions, all of which are issues in need of systemic attention in a joint environment.

The Department of Defense Cyber Strategy of April 2015 presents a broad policy, goals, and implementation objectives for the Department of Defense in cyberspace. It will help guide service components and the joint acquisitions community to develop the cyber capabilities and capacity needed in the newly defined cyber domain. The majority of the strategy is typical department level policy based on accelerating research and development efforts, drawing upon the expertise of the private sector, and concepts of organization. The new Cyber Mission Force (CMF) is described in the strategy. The CMF is an organization of teams with cyber capabilities to support DoD missions, but it is not mentioned how they will be linked to joint operations. The CMF is a unique structure and there is currently no doctrinal basis for their composition and

capabilities. Our Joint Task Forces need effective doctrine to employ the CMF teams when they deploy with them to conduct operations.[18]

The United States Marine Corps has created a concept called the MAGTF Cyberspace and Electronic Warfare Coordination Cell (CEWCC) with many considerations that can contribute to doctrine for joint operations, but it is a concept with a great deal of service-specific elements that need translation to be effective in joint doctrine. The MAGTF CEWCC's "Cyberspace/EMS Coordination Matrix" and MAGTF CEWCC personnel roles/responsibilities are interesting ideas that can possibly contribute to similar concepts in joint doctrine.[19] It also emphasizes that "the Marine Corps should employ cyberspace and EMS related expertise and systems holistically in support of all warfighting functions and objectives, and in accordance with the principles of combined arms maneuver."[20] The MAGTF CEWCC is a concept applicable only at the subordinate Marine Corps Service Component level of a JTF consisting of multiple service components. In the majority of military operations the MAGTF will not be operating in isolation from other service components in the JTF. A similar overarching joint doctrine on Cyber C2 needs to provide the primary direction for the service components to provide capabilities such as these coordination cells that will be interoperable in the JTF.

Referencing existing doctrine that is not specific to cyberspace will also help in the development of effective new doctrine for cyberspace. *Marine Corps Doctrinal Publication 6, Command and Control* provides a theory on command and control systems with elements that correlate to the three layers of cyberspace defined in JP 3-12(R).[21] Analyzing the theory and how it applies to cyberspace can help define a "cyber C2 system" for the Joint Task Force Commander to achieve better C2 of cyberspace.

Situational awareness is a concept thoroughly documented in existing doctrine. *Joint Publication 1, Doctrine for the Armed Forces of the United States* provides the definition and theory on use of situational awareness for commanders conducting joint operations.[22] Situational

awareness is also the underlying concept for the Common Operational Picture (COP). *CJCSI 3151* provides the reporting requirements for commanders' air, land, and maritime pictures.[23] Doctrine is lacking that effectively describes what cyber situational awareness is and what a cyber picture should consist of in the COP.

Other doctrinal publications such as *JP 3-0 Joint Operations* and *MCWP 3-4.1 MAGTF Command and Control* provide the basis for how command and control relates to the Joint Task Force and how C2 systems support operations.[24] They do not address command and control of cyberspace or how cyberspace supports operations.

An effort is required to create new doctrine that would be more effective for joint operations. Many existing joint publications and other doctrine do not take into consideration the new concepts of the cyber domain as presented in the writings of those such as Lynn, Lindsay, Lambeth, Hunter, and Bonner. The doctrine that does exist fails to provide a clear and useful common understanding of what cyberspace means to the Joint Task Force. The area of doctrine most lacking, and as this research argues is most important, is how the Commander of the Joint Task Force achieves command and control when including operations related to cyberspace.

The Cyber C2 System

In order to gain better command and control of the cyber battlespace, a Joint Task Force Commander first needs doctrine for his/her cyber command and control system. This doctrine will contribute to the interoperability of the JTF's service components in cyberspace. The existing doctrine of command and control (C2) describes C2 and the components of C2 systems. A comparison of the components of C2 in the existing doctrine with what is required in the commander's cyber battlespace will provide suggestions for what would define a "Cyber C2 System." While cyberspace is comprised of physical networks, logical networks, and cyber personas, the Joint Task Force cyber command and control system consists of people,

information, and support structure. Doctrine needs to provide the basis of what the people, information, and support structure provide to command and control of cyberspace.

The concept of "command and control" has been one of the basic warfighting functions for hundreds of years. In current U.S. DoD Joint Doctrine, command and control is a function common to all operations at the tactical, operational, and strategic levels; "C2 encompasses the exercise of authority and direction by a commander over assigned and attached forces to accomplish the mission. The JFC provides operational vision, guidance, and direction to the joint force."[25] In modern warfare command and control has often been associated with communications systems, as technological advances have resulted in communications equipment with significant capabilities that enable command and control. United States Marine Corps doctrine succinctly describes command and control as "the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken."[26] Considering the United States conducts operations as a Joint Force, the command and control of the Joint Task Force is the ultimate product that validates the usefulness of doctrine on command and control.

Command and control exists within military organizations as a system with interacting components. To effectively describe this interacting system of actions and feedback, Marine Corps doctrine states that a C2 system consists of people, information, and support structures.[27] First, people are the human element of the system. They are the commanders making decisions and the subordinates taking action. Second, the information element is what is being communicated or interpreted in the battlespace. It is the sounds, imagery, text, or numbers that either create situational awareness or communicate actions in the battlespace.[28] Third, the command and control support structure element is everything that enables the people element to use the information element in the system. This includes the physical items such as radios, computers, servers, networking hardware, data centers, operations centers, and organizations, as

well as the training and operating procedures they have.[29] The current doctrine on cyberspace does not effectively describe how the people, information, and support structures operate in the cyber domain as a cyber C2 system, as has been done in the existing C2 doctrine.

In a cyber command and control system the commander needs to be able to visualize what needs to be done in the cyber domain and see to it that appropriate actions are taken. Defining cyberspace is the first requirement for visualization. JP 3-12R *Cyberspace Operations* describes three different layers of cyberspace where cyber operations can be conducted. There is the physical network layer, the logical network layer, and the cyber persona layer. The physical network is self explanatory; it is the physical layer which is comprised of the software, hardware, cables, network equipment, etc. It is also the geographic component of cyberspace.[30] It reads: "The logical network layer consists of those elements of the network that are related to one another in a way that is abstracted from the physical network, i.e., the form or relationships are not tied to an individual, specific path, or node."[31] The third and final layer of cyberspace is the cyber-persona layer. It is the layer that combines the physical and logical connections "to develop a digital representation of an individual or entity identity in cyberspace. The cyber-persona layer consists of the people actually on the network."[32]

With an understanding of the components of a C2 System and a definition of cyberspace, the elements of the cyber C2 system can be defined in relation to cyberspace. The people, information, and C2 support structure that comprise a C2 system are analogous to the cyber personas, logical networks, and physical networks that are layered in cyberspace.

The element of people in a C2 system is analogous to the cyber-persona layer of cyberspace. The cyber-persona is where the human element operates in cyberspace. Perhaps one reason why the cyber domain is so critical to modern military operations lies in the fact that the human C2 element exists in the most abstracted and networked layer of cyberspace. The Joint Force Commander's C2 system is comprised of the commander persona, operator personas,

network/security/information assurance personnel, watch officers, and information/knowledge management officers. The logical network layer is comparable to the information element of command and control in that it is where information makes the logical connection between people and the physical domain in cyberspace. The physical network layer is comparable to the command and control support structure. It includes the hardware, software, input/output devices, power supplies, and the terrestrial cable, wireless, and space networks.

The authors of *JP 3-12(R)* chose to describe cyberspace as the three network layers and consequently a derivative of the C2 system concept. This places extreme significance on the correlation of the service components' C2 systems to the Joint Task Force cyber C2 system. When analyzing this correlation of the elements that comprise a command and control system with the overlapping network layers that define cyberspace, one can make several determinations. First, that command and control is the most important concept in the cyber domain. Second, that the cyber domain is an expansive command and control system. It is the product of the evolution of command and control technology within the military.

Additionally, the physical network is a key element of the Joint Task Force's cyber battlespace because it is the geographical representation of cyberspace. All links and nodes reside in the physical domain. With this consideration the Joint Task Force Commander can determine requirements for the Joint Task Force's cyber situational awareness systems and geospatial information systems that contribute to command and control of the cyber battlespace. Updating existing doctrine on C2 systems to include cyberspace, and creating new doctrine for cyber C2 systems will lead to a common understanding of the cyber domain in the JTF's C2 system. It will also be the foundation of doctrine for cyber situational awareness systems.

Cyber Situational Awareness

In order to better gain command and control of cyberspace, a Joint Task Force Commander needs to develop situational awareness of the cyber domain in relation to the physical domains, and visualize the interoperability of air, land, maritime, and cyber components. Joint doctrine, Chairman of the Joints Chiefs of Staff Instructions (CJCSI), and DoD programs of record have provided command and control capabilities and direction for the Combatant Commanders, Services, and Joint Forces in the past. In the last decade, situational awareness software has become a standard method for joint forces to exercise command and control with geospatial information systems among the land, maritime, air, and space domains. Situational awareness of today's Joint Force battlespace, to include cyberspace, can be achieved by incorporating and managing a cyber picture in conjunction with the land, maritime, air, and space pictures that represent the warfighting domains in the Common Operational Picture (COP). An effective cyber picture will graphically portray the actions in cyberspace as they relate to the geographical representation of forces in the physical domains.

Situational awareness (SA) is "a prerequisite for commanders anticipating opportunities and challenges. True situational understanding should be the basis for all decision makers. Knowledge of friendly capabilities and adversary capabilities, intentions, and likely COAs enables commanders to focus joint efforts where they best and most directly contribute to achieving objectives."[33] The Common Operational Picture is a doctrinal tool for joint forces that provides a graphical geospatial visualization of the battlespace which consists of a basic chart (C2PC, ICSF, or Agile Client) which can be a map or imagery of the battlespace. Joint operations centers manage a COP over the charts to display units, air platforms, maritime platforms, overlays, battlespace coordination measures or other "tracks" for friendly, threat/adversary, neutral, and ambiguous forces. The forces that provide cyber capability to joint operations, and the operations they are conducting need to be incorporated into the COP.[34]

The Global Command and Control System-Joint (GCCS-J) is the program of record for command and control of joint operations, and within the GCCS-J program a Global COP capability is provided. The COP reporting requirements for the GCCS-J are outlined by the Chairman of the Joint Chiefs of Staff in *CJSI 3151.01C*. The GCCS-J program is used globally by the Combatant Commanders, Services Chiefs, Service Component Commanders and other Joint Task Forces for exercising command and control and providing situational awareness of activities amongst joint forces and to the senior military leadership and the Joint Staff. The Global COP currently provides situational awareness at the operational level with hundreds of capabilities in the land, air, space and maritime domains; such as theater ballistic missile alerts, friendly force tracking, air tasking order information, the threat/adversary "red picture", etc. There are tracks for airplanes, ships, units, facilities, and FBCB2 vehicle tracks, but there is no standard software interface or package in GCCS-J to display the "cyber picture." The effects of cyberspace operations conducted by the JTF cannot be shared with adjacent or reported to higher without situational awareness which is achieved by joint forces through the COP.[35]

Joint doctrine has already identified the need for a cyberspace COP in *JP 3-12R Cyberspace Operations*:

> A common operational picture (COP) for cyberspace facilitates C2 of CO and real-time comprehensive SA. A cyberspace COP should include the ability to rapidly fuse, correlate, and display data from global network sensors to deliver a reliable picture of friendly, neutral, and adversary networks, including their physical locations and activities. In addition, the cyberspace COP should support real-time threat and event data from myriad sources (i.e., DOD, IC, interagency, private industry, and international partners) and improve commanders' abilities to identify, monitor, characterize, track, locate and take action in response to cyberspace activity as it occurs both globally for USSTRATCOM/USCYBERCOM and within the AOR for the GCC.[36]
> (*JP 3-12R Cyberspace Operations*)

Cyberspace Operations fails to identify that the cyberspace COP should be incorporated as a component of the GCCS-J COP. This cyberspace COP would be most effective in providing cross-domain synergy as a "cyber picture" in the GCCS-J Global COP which is the program of record for situational awareness among the joint forces for all warfighting domains. Operations in cyberspace are joint operations and they should be part of the GCCS-J program of

record for Joint C2. All of the doctrinal concepts associated with the cyber domain, to include the factors mentioned in *Cyberspace Operations*, need to be applied as a doctrinal tool in the GCCS-J program used by the joint forces. In addition to *Cyberspace Operations'* description of what a cyber COP should consist of, cyber SA and visualization of the cyber COP can be discussed further.

To incorporate the cyber COP in the GCCS-J Global COP, it would have to first involve a geographical representation of the friendly cyber forces, threat/adversary cyber forces, and neutral cyber forces. The area of the Internet outside of the DoD network is commonly referred to as the DMZ, which could potentially be neutral or threat forces in the cyber COP. Part of the geographical representation would involve management of the physical location of the physical network layer. Based off the previous discussion of cyber C2 systems, the immediate, geographical, view of the physical network would primarily consist of nodes and links between the nodes. The basic principle of a blue/friendly force cyber picture is not new. Network status and monitoring tools have been available and heavily used for some time. Examples such as "What's up Gold©" or "Solar Winds©" allow network managers to enter in the IP addresses of the nodes on their network, configure where they are physically located in the visualization applications, and monitor the status (operational/degraded) of the assets on the network. It is essential that all forces monitor the status of operations in cyberspace because in the unconstrained nature of cyberspace, as mentioned by Benjamin Lambeth[37], a vulnerability or opportunity can have significant impact on the ability to accomplish the mission. A threat can attack and exploit vulnerabilities through cyberspace regardless of separations in time and space. Additionally, the systems depended upon to conduct the mission have become so complex that they require significant monitoring to prevent fragility.

The threat picture would be something that would need to be provided by the Intelligence Community(IC). One main problem is that the IC operates on networks for TS/SCI levels of

classification, and GCCS-J with the Global COP is managed at the secret level on SIPRNET. This problem has solutions though because the IC has always had to operate on their networks and provide reports saying "the threat/adversary/enemy is here… they are doing this…" The GCCS-J program developed a component specifically for intelligence support to the COP with their Integrated Imagery and Intelligence (I3) software packages. The GCCS-J I3 capabilities include JTT for target development and modernized integrated database (MIDB).[38] MIDB is developed and managed by a program management office in the Defense Intelligence Agency (DIA). In 2015 GCCS-J version 5.0 was scheduled to be released and fielded with an enhanced capability for MIDB called the cyber network operations database (CNODB). At the design review the software developers provided concepts of the enhancement that included the ability to graphically display the links, nodes, and networks; and the database would allow the users to analyze additional track attributes that would contain more amplifying or abstract data. CNODB was just being designed as a database capability; there were no real sources of data to fill the database and actually employ CNODB at the time of the design review.[39]

There is the potential for applying technology to the geographic representation of the cyber COP that would allow amplifying data to be associated with the tracks for the nodes and links; this would potentially allow analysis of the correlation to logical networks and other more abstracted associations within cyberspace. The analysis at this level, in combination with fusion of the other intelligence and the other friendly force tracks, should result in cyber COP management with a graphic representation of the cyber persona layer. With a COP that represents all three layers of cyberspace the commander will have situational awareness of the friendly and threat forces' C2 systems in cyber space and "the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken."[40]

With SA of the cyber domain through a cyber picture within the COP, the JTF will effectively integrate C2 of the cyber domain within the physical warfighting domains because

cyber capabilities are now included in warfighting. Maintenance of the cyber picture will allow accurate portrayal of the information from the battlespace to be displayed in the chart on the wall of the Joint Operations Center, and ensure all JTF operations are monitored and coordinated. Additionally, the information in the cyber picture will be efficiently communicated to adjacent commands, and also reported to higher headquarters.

Command Relationships and Authorities

In order to better gain command and control of cyberspace that allows inter-service full-spectrum cyber operations to happen, a Joint Task Force Commander needs to fully understand and optimize command authorities and command relationships. In recent years there have been many new Department of Defense concepts and organizations designed to build cyber capability and capacity. There are also important considerations regarding the traditional organizations and processes related to the cyber domain, such as Department of Defense information assurance programs, network certification and accreditation, and network defense.

A Joint Task Force needs to be integrated into the existing cyber command relationships in DoD, review command authorities, and organize a JTF with a C2 structure outlining command authorities in cyberspace. The current Cyberspace C2 organizational construct in *JP 3-12R Cyberspace Operations* is outdated, and incorrect. Figure 1 below is the outdated construct; it does not include new cyber organizations that are part of the CMF, and the command authorities are inaccurate.[41]

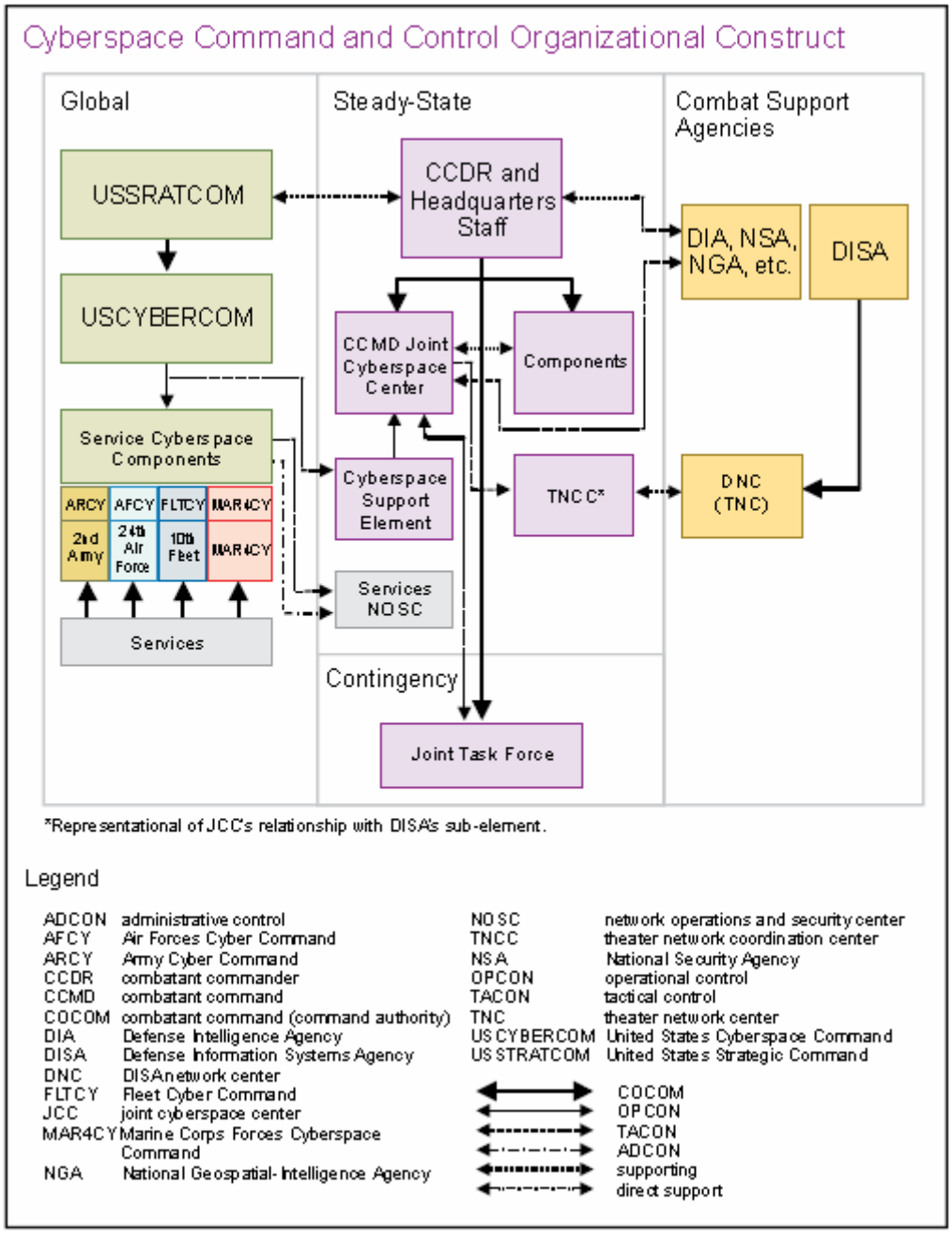

Figure 1. Cyberspace Command and Control Organizational Construct

(JP 3-12 *Cyberspace Operations* IV-8, 5 Feb. 2013

Combatant commanders and joint force commanders have the original authority to command U.S. military forces. There are several doctrinal concepts which facilitate the delegation of command authorities (also referred to as command relationships) to subordinate commanders that allow them to have operational control or tactical control over assigned forces, or supporting relationships.[42] The Secretary of Defense recently created a new command

authority specifically for cyberspace operations on 13 November 2014. Directive authority for cyberspace operations (DACO) gives the Commander of United States Cyber Command, and the subordinate Joint Force Headquarters-DODIN Commander DACO to "issue orders and directives to all DoD components for directing the execution of global DODIN operations and Defensive Cyber Operations – Internal Defensive Measures to compel unity of action to secure, operate, and defend the DODIN."[43] This authority was specifically created to address the issue of tasking Combat Support Agencies, and other DoD agencies for DCO-IDM and DODIN operations. DACO gives the tasking authority (TACON) equivalent to Title 10 organizations.[44] Service components are addressing the issue of tasking commands outside the traditional chain of command as well. The Commander, MARFORCYBER has had a DACO authority delegated to him over Marine Corps operating forces, reserves, and the supporting establishment via a MCEN unification message.[45] This new command authority of DACO (see Figure 2.) needs to be part of new doctrine for command and control of cyberspace, and existing doctrine needs to be updated.

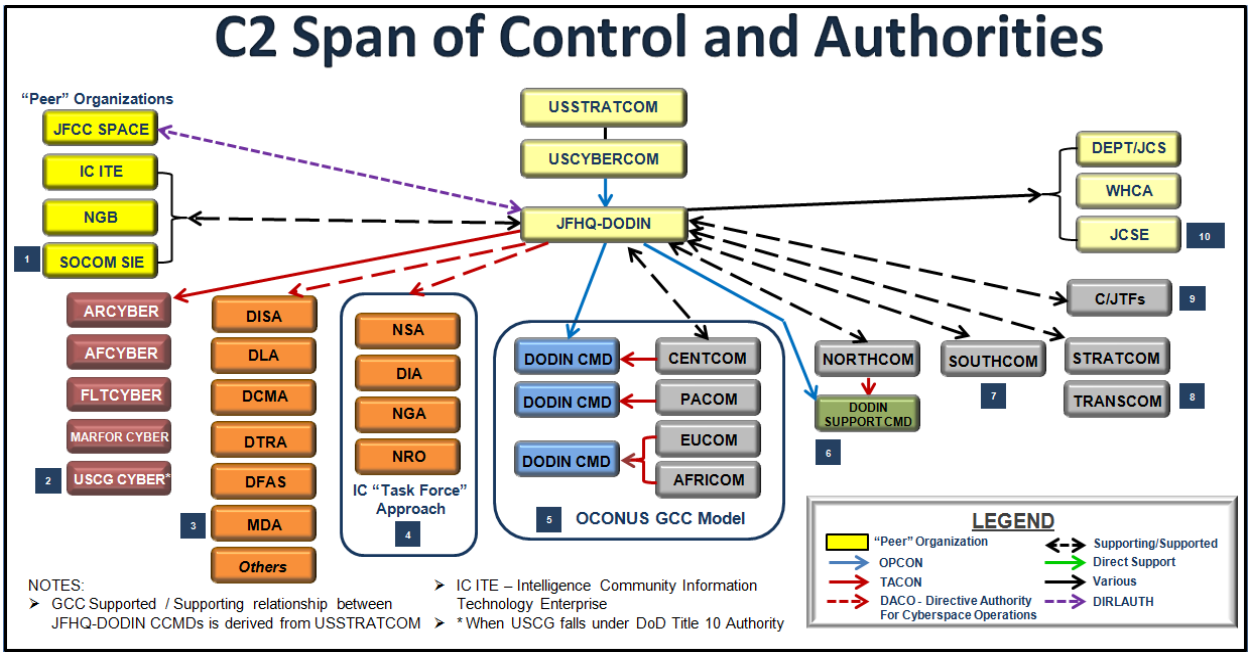

Figure 2. C2 Span of Control and Authorities

(Joint Force Headquarters-DODIN Mission Brief, 2 Sept. 2015)

The DACO authority ties together the traditional command and control relationships among commands within the air, land, maritime, and space domains with the cyber domain. There are traditional "authorities" or processes involved with operating in the DODIN; the Defense Information Assurance Certification and Accreditation Process (DIACAP) manages the authority to operate (the main certification is literally the "authority to operate [ATO]") on a defense information systems network. A network has to meet security requirements, information assurance requirements, use approved software, and have certified network management in order to be certified and receive an ATO. The same applies to DoD software programs; before they are approved for release and operation on the networks they are scanned, tested, and certified to receive an ATO. The ATO process is ultimately the risk assessment that determines whether our information systems have been secured from vulnerabilities to an acceptable level to operate in the cyber domain.[46]

Much of the network accreditation will take place at the higher headquarters of the Joint Task Force, and the JTF will likely be a subordinate under the DACO authority of the Geographic Combatant Commander (GCC). For cyberspace operations, the organization at the GCC would be the Combat Command Joint Cyberspace Centers. For a service specific system or network used by the Joint Task Force, there would be DACO relationships with the service JFHQ-Cyber.

The Joint Task Force Commander would also want to create a command and control construct within the JTF that incorporates elements representing the JTF cyber domain. This involves forming a Joint Task Force cyber C2 system with people, or cyber-personas, in effective command relationships within the JTF.

The traditional Joint Task Force organization has elements that already represent the categories of cyber support. If all elements were to maintain status quo given cyber capabilities, the Fires Section in the J-3 would manage offensive cyber capabilities, the Communications

Section in the J-6 would manage defensive cyber capabilities, and the Information Management Officer/Knowledge Management Officer would manage the DoD Information Network operations. Considering the relationship between the JTF C2 structure and the concept of a Joint Task Force cyber C2 system previously discussed, there may be the need to evaluate whether specific people, elements, or cyber-personas such as a "J-3 Cyber" needs to be created for C2 of the cyber battlespace. In addition to an individual whose sole responsibility is the Joint Task Force cyber battlespace, the Joint Task Force cyber C2 system can provide support across all warfighting functions. Since Cyberspace is a domain in which all forces operate, there are offensive and defensive cyber considerations for each warfighting function. It is this level of interconnectedness and reliance on information systems that has created as Deputy Secretary Lynn states "the Cyber Domain."[47]

Cyber Support to the Warfighting Functions

In order to better gain command and control of cyberspace, a Joint Task Force Commander needs his/her staff to consider cyber support to the warfighting functions. In the past, the capabilities that are now considered cyber capabilities were grouped into one of the warfighting functions. For instance, they were basically considered to be part of the fires function with electronic warfare, or using information systems and internetworking through the C2 function and defending the network through either the C2 function or force protection. To effectively command and control the cyber battle space, cyber considerations specific to the operation need to be identified in the planning process, and this can be achieved with updated planning products, possibly doctrinal templates, that include cyber support across all warfighting functions.

There are six warfighting functions in joint operations. A Joint Task Force conducts planning with consideration to these warfighting functions. The functions are fires, command and control, maneuver, force protection, sustainment/logistics, and intelligence. In Marine Corps

Warfighting Publication 3-40.1 *Marine Air-Ground Task Force C2*, key MAGTF information systems that support generic MAGTF operations are described in conjunction with the warfighting functions. The warfighting functions are categorized and key information systems are detailed for each function. Some examples include detailing why AFATDS is important to the fires function, MDSSII and JOPES' functionality within the logistics function.[48] This is a good concept to identify in doctrine that key information systems should be broken down by function with the MAGTF/Joint Task Force, but as Commander Huntley mentions;[49] identifying specific systems in doctrine can get outdated quickly with today's joint force (given the frequently changing nature of cyber capabilities). Many of the specific systems in the current doctrine have been replaced (JOPES) and many key systems released after the publication are omitted (Global Combat Support System, for instance).

As previously noted, when describing the significance of technological development to the cyber C2 system, the same principle applies across all the warfighting functions. Our logistics, force protection, maneuver, fires, and intelligence systems have developed to take advantage of the information technologies that have evolved into the cyber domain. Cyberspace provides an unprecedented level of efficiency and effectiveness to each warfighting function. It is important to assure the DODIN operations that enable these functions. The reliance on cyberspace also introduces vulnerabilities by introducing the functions to a complex and internetworked system. It is important that vulnerabilities are identified, defended, and redundant capabilities available as a backup for each function.

There are three broad categories of cyber support that would be available to a Joint Task Force. First, DODIN operations would be ensuring the full use of cyberspace through the entire spectrum of information systems and information networks available to the joint force. An example of this would be taking a task someone in the joint force used to do with pencil and paper and having them do it in a more timely, accurate, and efficient manner electronically. The

email itself is routine use of cyberspace, but enabling them with capable email and assuring its reliability is DODIN operations. The second category is Defense Cyber Operations (DCO). DCO can be broadly defined as defending the network, and it includes two subcategories of defensive operations; DCO internal defense measures (DCO-IDM) and DCO response actions (DCO-RA). JP 3-12R states that DCO should be prioritized, with a redundant set of primary/secondary/tertiary communications.[50] The third category is Offensive Cyber Operations (OCO). "OCO are CO intended to project power by the application of force in and through cyberspace."[51]

Doctrine for the Joint Task Force should present a process for cyber support to the warfighting functions of each operation, not a doctrinal procedure of which capability supports each warfighting function. The process would allow the most effective cyber support tailored to each unique joint operation. This would provide more useful and flexible doctrine for joint forces and prevent referencing outdated doctrine (such as MCWP 3-40.1) in the planning of operations; or worse, the actual use of an outdated and vulnerable system in cyberspace.

The process for cyber support to the warfighting functions should involve the representative from each function in an operational planning team (OPT), or the staff assigned to the Joint Task Force. First, each function can identify the key information systems and DODIN functions required for them to conduct the mission and the redundant/backup method to conduct that function. Second, the capabilities should be prioritized with any single threaded (no backup) capabilities identified for the DCO priorities and reinforcement. Finally, any OCO support that would improve the functions ability to accomplish the mission would be identified. While at first it seems OCO would be primarily used in support of the JTF's fires function, there are cases where OCO may support other functions; for example, the C2 function requesting OCO to target adversary electronic warfare systems.

The service cyber components have been using some unofficial methods for cyber planning support, but there is no standardization and no agreed upon doctrine. By using a standard method of applying the three types of cyberspace operations to the planning process of the Joint Task Force such as the suggested one along the lines of warfighting functions, the Joint Task Force Commander will have better command and control of the JTF cyber battlespace. The JTF's operations will have a combination of the full spectrum of its functions merged with the full spectrum of CO in its cyber domain; the commander will be able to see this domain along functional lines and ensure those functions are taking place.

Conclusions

Through the course of history to today's current military operations, the characteristics of the battlespace have been influenced by technology. The capabilities of the United States military have evolved to the point where they are thoroughly immersed with technology and interconnected information systems. They are also heavily reliant upon this technology. Command and control has always been a critical warfighting function, and it has been primarily through the technological advancement and innovation in command and control systems that the cyber warfighting domain has emerged. In many aspects, the military cyber domain represents the greatest military C2 system of people, information, and support structures.

The cyber domain is unique in comparison to the other physical domains, as it is a reflection of how humans interact in the information environment. Each branch of service provides unique capabilities to the U.S. military, and these capabilities include the technology, information systems, and C2 systems that have enhanced their operations. These capabilities now include the cyber capabilities that will accompany service components as they are employed to conduct operations as part of a joint force.

Effective doctrine is needed for command and control of the cyber battlespace for the Joint Task Forces to be effective in terms of utilizing cyber power in military operations.

Consequently, service-specific cyber capabilities need to be interoperable and able to support how the United States conducts military operations in the Joint Environment.

The military does not get on the same page until doctrine is complete and effective in describing how to conduct operations. General DePuy's stance on the importance of doctrinal concepts as a guide to action led to the progression of doctrine and effective operational concepts for the U.S. Army in the timeframe following the Vietnam War.[52] Similarly, doctrine on the C2 of cyberspace operations needs to progress and expand military thinking on cyberspace, and develop concepts that will lead actions in the joint forces' next war in the cyber domain.

The doctrine published by the Department of Defense on the cyber domain and cyberspace operations has defined the strategic goals in cyberspace, and described some of the terms associated with the domain and cyber operations. The concept of cyberspace is relatively new, and the current doctrine is inadequate in describing how command and control of the cyber domain is attained in the Joint Task Forces' battlespace. The most useful doctrine will help the commanders visualize how to gain effective C2 in cyberspace, and also provide guidelines for development and common understanding to the service components that will be supporting them. Useful doctrine would also educate and inform the U.S. military on new concepts related to cyberspace. The command relationships and command authorities are of particular importance to C2. The traditional command relationships that are well understood throughout the DoD need to be translated effectively to the new command relationships in the Cyber C2 Construct (Figure 2). Additionally, the traditional command authorities need to be de-conflicted with traditional authorities uniquely related to cyberspace such as the DIACAP and the ATO.

There are several specific recommendations that can be made to address the existing doctrine being inadequate or outdated, and the further articulation of new concepts. The most apparent solution is a publication specifically regarding C2 and cyber operations. The creation of "*Joint Publication 3-3X Command and Control for Joint Cyber Operations*" would be a

similar concept to the joint doctrine on C2 of the physical domains, and would compliment *JP 3-30, 3-31,* and *3-32*.

The Global Command and Control System-Joint system of record for C2 of joint operations needs to be updated as well. The cyber domain needs to be communicated as a cyber picture along with the already existing land, maritime, and air pictures that comprise the common operational picture. The requirements for the cyber picture would need to be based off of an updated instruction, or updated version of *CJCSI 3151*.

In addition to creating new doctrine, the existing doctrine needs to be updated to reflect accurate C2 relationships and the composition of the Cyber Mission Force. The new DACO command authority also needs to be defined in doctrine and understood in order for it to be effective. The DACO authority has been issued by the Secretary of Defense via a modification to an execute order, but it is missing from all the existing doctrine on cyberspace and command authorities.

Planning support tools for cyber considerations should also be included in joint doctrine. A Joint Task Force staff conducting planning for operations, or a service component referencing doctrine, will benefit from general guidelines for providing OCO, DCO, and DODIN Ops support across all joint warfighting functions.

Future operations in cyberspace present both a great opportunity to have more effective JTF operations (representing cyber at the operational level), and it also presents a great threat where failing to address vulnerabilities can have drastic consequences. With the relatively new concepts of the cyber domain and cyber power, proactively providing useful doctrine on cyberspace will allow the creation of interoperable joint forces in the cyber domain.

Ultimately, this research indentifies several implications on the significance of C2 in cyberspace to the Joint Task Force, and the service components that provide them capabilities. First, cyberspace is the supreme C2 system. Understanding the foundations of command and

control systems provides a clear vision of how the three network layers of cyberspace exist. This visualization is useful as there are no tangible distinctions in cyberspace as there are in the physical domains. Second, the application of doctrinal tools such as the common operational picture and reporting requirements for a cyber picture will help provide situational awareness of cyberspace. Third, the new command relationships and authorities within cyberspace need to be clearly identified and understood by all U.S. military forces. This will allow the necessary tasking to take place and reduce confusion that could lead to vulnerability in the cyber battlespace. Lastly, all of the joint warfighting functions require systems that have been developed to take full advantage of the benefits of technology. Cyber power thus provides significant support to all warfighting functions.

Endnotes

[1] Joint Staff, *Joint Publication 3-12 Cyberspace Operations*, (5 February 2013), I-I.

[2] James Stavridis and David Weinstein, "Time for a U.S. Cyber Force," *Proceedings Magazine*, Vol. 1 40/1/1,331 (January 2014): http://www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force.

[3] Ash Carter, "Remarks by Secretary Carter to U.S. Cyber Command Workforce at Fort Meade, Maryland" (speech, United States Cyber Command, Fort Meade, MD, March 13, 2015).

[4] Kenneth F. McKenzie Jr., "On the Verge of a New Era: The Marine Corps and Maneuver Warfare," *Marine Corps Gazette*, Vol. 77, 7, (July 1993): 64-66.

[5] Lincoln E. Bonner III, "Cyber Power in 21st-Century Joint Warfare," *Joint Force Quarterly*, Issue 74, (3rd Quarter 2014): 103.

[6] Armed Forces Staff College, *Joint Command and Control Warfare Staff Officer Course Student Text*, (Norfolk, VA: Armed Forces Staff College, September 1995) 1-1.

[7] Armed Forces Staff College, *Joint Command and Control Warfare Staff Officer Course Student Text*, (Norfolk, VA: Armed Forces Staff College, September 1995) 1-1 – 1-7.

[8] William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, Vol. 89, Issue 5 (Sept-Oct 2010): 99.

[9] William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, Vol. 89, Issue 5 (Sept-Oct 2010): 99-108.

[10] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3 (2013): 365-404.

[11] Benjamin S. Lambeth, "Airpower, Spacepowers, and Cyberpower," *Joint Force Quarterly*, Issue 60, (1st Quarter 2011): 50.

[12] Todd C. Huntley, "Controlling the Use of Force in Cyberspace: The Application of the Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare," *Naval Law Review*, Vol 60. (2010): 4.

[13] Todd C. Huntley, "Controlling the Use of Force in Cyberspace: The Application of the Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare," *Naval Law Review*, Vol 60. (2010): 6.

[14] Lincoln E. Bonner III, "Cyber Power in 21st-Century Joint Warfare," *Joint Force Quarterly*, Issue 74, (3rd Quarter 2014): 103-109.

[15] Lincoln E. Bonner III, "Cyber Power in 21st-Century Joint Warfare," *Joint Force Quarterly*, Issue 74, (3rd Quarter 2014): 102-109.

[16] *Department of Defense Reorganization Act of 1986*, Committee on the Armed Services, United States Senate, 99th Cong., Report 99-280. (14 April 1986) 7-9.

[17] Joint Staff, *Joint Publication 3-12 Cyberspace Operations*, (5 February 2013), IV-7.

[18] Department of Defense, *The Department of Defense Cyber Strategy*, (April 2015) 1-33. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[19] Headquarters US Marine Corps, *MAGTF Cyberspace and Electronic Warfare Coordination Cell (CEWCC) Concept*. (Washington, DC: Headquarters US Marine Corps, 1 May 2014), (FOUO), 1-8.

[20] Headquarters US Marine Corps, *MAGTF Cyberspace and Electronic Warfare Coordination Cell (CEWCC) Concept*. (Washington, DC: Headquarters US Marine Corps, 1 May 2014), (FOUO), 2.

[21] Headquarters US Marine Corps, *Command and Control*. MCDP 6 (Washington, DC: Headquarters US Marine Corps, October 1996), 47-54.

[22] Joint Staff, *Joint Publication 1 Doctrine for the Armed Forces of the United States*, (25 March 2013), V-17.

[23] Joint Staff, *Chairman of the Joint Chiefs of Staff Instruction 3151.01B Global Command and Control System Common Operational Picture Reporting Requirements*, (31 October 2008), 2-6.

[24] Headquarters US Marine Corps, *Marine Air-Ground Task Force Command and Control*, MCWP 3-40.1 (Washington, DC: Headquarters US Marine Corps, 17 March 2003), 1-1 -9-8.

[25] Joint Staff, *Joint Publication 3-0 Joint Operations*, (11 August 2011), III-2.

[26] Headquarters US Marine Corps, *Command and Control*. MCDP 6 (Washington, DC: Headquarters US Marine Corps, October 1996), 37.

[27] Headquarters US Marine Corps, *Command and Control*. MCDP 6 (Washington, DC: Headquarters US Marine Corps, October 1996), 47.

[28] Headquarters US Marine Corps, *Command and Control*. MCDP 6 (Washington, DC: Headquarters US Marine Corps, October 1996), 49.

[29] Headquarters US Marine Corps, *Command and Control*. MCDP 6 (Washington, DC: Headquarters US Marine Corps, October 1996), 51.

[30] Joint Staff, *Joint Publication 3-12 Cyberspace Operations*, (5 February 2013), I-3.

[31] Joint Staff, *Joint Publication 3-12 Cyberspace Operations*, (5 February 2013), I-2.

[32] Joint Staff, *Joint Publication 3-12 Cyberspace Operations*, (5 February 2013), I-3.

[33] Joint Staff, *Joint Publication 1 Doctrine for the Armed Forces of the United States*, (25 March 2013), V-17.

[34] Joint Staff, *Chairman of the Joint Chiefs of Staff Instruction 3151.01B Global Command and Control System Common Operational Picture Reporting Requirements*, (31 October 2008), 1-5.

[35] Joint Staff, *Chairman of the Joint Chiefs of Staff Instruction 3151.01B Global Command and Control System Common Operational Picture Reporting Requirements*, (31 October 2008), 2-6.

[36] Joint Staff, *Joint Publication 3-12 Cyberspace Operations*, (5 February 2013), II-8.

[37] Benjamin S. Lambeth, "Airpower, Spacepowers, and Cyberpower," *Joint Force Quarterly*, Issue 60, (1st Quarter 2011): 51.

[38] Joint Staff, *Chairman of the Joint Chiefs of Staff Instruction 3151.01B Global Command and Control System Common Operational Picture Reporting Requirements*, (31 October 2008), A-6.

[39] *Global Command and Control System-Joint Release Version 5.0 Critical Design Review*, Defense Information Systems Agency, (June 2013).

[40] Headquarters US Marine Corps, *Command and Control*. MCDP 6 (Washington, DC: Headquarters US Marine Corps, October 1996), 37.

[41] Joint Staff, *Joint Publication 3-12 Cyberspace Operations*, (5 February 2013), IV-8.

[42] Joint Staff, *Joint Publication 3-0 Joint Operations*, (11 August 2011), III-3.

[43] Secretary of Defense, *Modification to Cyberspace C2 Execute Order*, November 13, 2014.

[44] Gregory Wynn, Joint Force Headquarters-DODIN J-53, personal email to author, March 17, 2016.

[45] Matthew Limbert, *SIG Scouting Report for the week of 7 Dec 2015,* (Washington DC: Headquarters, United States Marine Corps, Strategic Initiatives Group, December 2015): 3.

[46] U.S. Department of Defense. *Defense Information Assurance Certification and Accreditation Process* (Washington, DC: Personnel Readiness and Information Management, June 2011), www.prim.osd.mil/Documents/DIACAP_Slick_Sheet.pdf.

[47] William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, Vol. 89, Issue 5 (Sept-Oct 2010): 97.

[48] Headquarters US Marine Corps, *Marine Air-Ground Task Force Command and Control*, MCWP 3-40.1 (Washington, DC: Headquarters US Marine Corps, 17 March 2003), 8-8.

[49] Todd C. Huntley, "Controlling the Use of Force in Cyberspace: The Application of the Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare," *Naval Law Review*, Vol 60. (2010): 6.

[50] Joint Staff, *Joint Publication 3-12 Cyberspace Operations*, (5 February 2013), I-2.

[51] Joint Staff, *Joint Publication 3-12 Cyberspace Operations*, (5 February 2013), II-2.

[47] Richard M. Swain, "Filling the Void: The Operational Art and the U.S. Army," In *The Operational Art: Developments in the Theories of War*, ed. B.J.C. McKercher and Michael A. Hennessy, (Westport, Conn: Praeger Press, 1996) 150-166.

Bibliography.

Armed Forces Staff College. *Joint Command and Control Warfare Staff Officer Course Student Text*. Norfolk, VA: Armed Forces Staff College, September 1995.

Bonner, E. Lincoln III. "Cyber Power in 21st-Century Joint Warfare." *Joint Force Quarterly*, Issue 74, (3rd Quarter 2014): 102-109.

Carafano, James J. "Mastering the Art of Wiki: Understanding Social Networking and National Strategy." *Joint Force Quarterly*, Issue 60, (1st Quarter 2011): 73-78.

Carter, Ash. "Remarks by Secretary Carter to U.S. Cyber Command Workforce at Fort Meade, Maryland." Speech. United States Cyber Command, Fort Meade, MD, March 13, 2015.

Defense Information Systems Agency. *Global Command and Control System-Joint Release Version 5.0 Critical Design Review*. June 2013.

Department of Defense. *The Department of Defense Cyber Strategy*. April 2015. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Headquarters US Marine Corps. *MAGTF Cyberspace and Electronic Warfare Coordination Cell (CEWCC) Concept*. Washington, DC: Headquarters US Marine Corps, 1 May 2014 (FOUO).

Headquarters US Marine Corps. *Command and Control*. MCDP 6. Washington, DC: Headquarters US Marine Corps, October 1996.

Headquarters US Marine Corps. *Marine Air-Ground Task Force Command and Control*. MCWP 3-40.1. Washington, DC: Headquarters US Marine Corps, 17 March 2003.

Hughes, Rex. "A Treaty for Cyberspace." *International Affairs*, 86:2 (2010): 523-541.

Huntley, Todd C. "Controlling the Use of Force in Cyberspace: The Application of the Application of the Law of Armed Conflict During a Time of Fundamental Change in The Nature of Warfare." *Naval Law Review*, Vol 60. (2010): 1-40.

Joint Force Headquarters DODIN. *JFHQ-DODIN Mission Brief*. PowerPoint Presentation. United States Cyber Command, Fort Meade, MD, 2 September 2015.

Joint Staff. *Chairman of the Joint Chiefs of Staff Instruction 3151.01B Global Command and Control System Common Operational Picture Reporting Requirements*, 31 October 2008.

Joint Staff. *Joint Publication 1 Doctrine for the Armed Forces of the United States*, 25 March 2013.

Joint Staff. *Joint Publication 3-0 Joint Operations*, 11 August 2011.

Joint Staff. *Joint Publication 3-12 Cyberspace Operations*, 5 February 2013.

Lambeth, Benjamin S. “Airpower, Spacepowers, and Cyberpower.” *Joint Force Quarterly*, Issue 60, (1st Quarter 2011): 46-53.

Limbert, Matthew. *SIG Scouting Report for the week of 7 Dec 2015*. Washington DC: Headquarters, United States Marine Corps, Strategic Initiatives Group, December 2015.

Lind, William S. “Defining maneuver warfare for the Marine Corps.” *Marine Corps Gazette*, Vol. 64, 3 (March 1980): 55-58.

Lind, William S.; Nightengale, Keith; Schmitt, John F.; Sutton, Joseph W.; Wilson, Gary I. “The Changing Face of War: Into the Fourth Generation.” *Marine Corps Gazette*, Vol. 73, 10 (Oct 1989): 22-26.

Lindsay, Jon R. “Stuxnet and the Limits of Cyber Warfare.” *Security Studies*, Vol. 22, No. 3 (2013): 365-404.

Lynn, William J. III. “Defending a New Domain.” *Foreign Affairs*, Vol. 89, Issue 5 (Sept-Oct 2010): 97-108.

McKenzie, Kenneth F. Jr. “On the Verge of a New Era: The Marine Corps and Maneuver Warfare.” *Marine Corps Gazette*, Vol. 77, 7 (July 1993): 63-67.

Secretary of Defense. *Modification to Cyberspace C2 Execute Order*. November 13, 2014.

Stavridis, James, and David Weinstein. “Time for a U.S. Cyber Force.” *Proceedings Magazine*, Vol. 1 40/1/1,331 (January 2014): http://www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force.

Swain, Richard M. “Filling the Void: The Operational Art and the U.S. Army.” In *The Operational Art: Developments in the Theories of War*, ed. B.J.C. McKercher and Michael A. Hennessy, 147-169. Westport, Conn: Praeger Press, 1996.

United States Senate. Committee on the Armed Services. *Department of Defense Reorganization Act of 1986*. 99th Cong. Report 99-280. (14 April 1986): 7-9.

U.S. Department of Defense. *Defense Information Assurance Certification and Accreditation Process*. Washington, DC: Personnel Readiness and Information Management, June 2011. www.prim.osd.mil/Documents/DIACAP_Slick_Sheet.pdf.

Wilson, G.I.; Wyly, Michael D.; Lind, William S.; Trainor, B.E. “The ‘Maneuver Warfare’ Concept.” *Marine Corps Gazette*, Vol.65, 4 (Apr 1981): 49-54.

Wynn, Gregory. Joint Force Headquarters-DODIN J-53. Personal email to author, March 17, 2016.