REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
27-10-2010	FINAL	

4. TITLE AND SUBTITLE

What and Where? Considerations for Command and Control of Cyberspace Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lt Col Robert L. Ramsden, USAF

Paper Advisor (if Any):

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

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

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

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

14. ABSTRACT

The Quadrennial Defense Review initiative to "centralize command of cyberspace operations" and the recent stand-up of U.S. Cyber Command lead to questions regarding the command and control of cyberspace operations. Given the inherent tension between a functional command structure and regional command structures, what are the implications? How should cyberspace operations be commanded and controlled? The problem we are trying to avoid, other than the negative aspects of competing objectives between commands, is the over-simplification of command architectures or over-centralization of command for all cyberspace operations. The argument furthered here is that a universal command and control structure should not be applied to all cyberspace operations. Effective command and control in the cyberspace domain should depend on what cyberspace operation is being executed and where in the cyberspace domain it is being performed. The appropriate centralization (what and where) is then informed by the objective being supported by that operation.

15. SUBJECT TERMS
Cyberspace, cyberspace operations, command and control, command relationships

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

NAVAL WAR COLLEGE
Newport, R.I.

WHAT AND WHERE? CONSIDERATIONS FOR COMMAND AND CONTROL OF CYBERSPACE OPERATIONS

by

Robert L. Ramsden

Lt Col, USAF

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: _____

27 October 2010

Contents

Abstract

What and Where? Considerations for Command and Control of Cyberspace Operations.

The Quadrennial Defense Review initiative to "centralize command of cyberspace operations" and the recent stand-up of U.S. Cyber Command lead to questions regarding the command and control of cyberspace operations. Given the inherent tension between a functional command structure and regional command structures, what are the implications? How should cyberspace operations be commanded and controlled? The problem we are trying to avoid, other than the negative aspects of competing objectives between commands, is the over-simplification of command architectures or over-centralization of command for all cyberspace operations. The argument furthered here is that a universal command and control structure should not be applied to all cyberspace operations. Effective command and control in the cyberspace domain should depend on what cyberspace operation is being executed and where in the cyberspace domain it is being performed. The appropriate centralization (what and where) is then informed by the objective being supported by that operation.

Introduction

"Centralize command of cyberspace operations. In an effort to organize and standardize cyber practices and operations more effectively, the Department is standing up U.S. Cyber Command (USCYBERCOM), a subunified command under U.S. Strategic Command, to lead, integrate and better coordinate the day-to-day defense, protection, and operation of DoD networks. USCYBERCOM will direct the operation and defense of DoD's information networks, and will prepare to, and when directed, conduct full spectrum cyberspace military operations."

Quadrennial Defense Review, February 2010

The excerpt above is one of four initiatives discussed in the Quadrennial Defense Review (QDR) to strengthen capabilities in cyberspace.[1] The title of this initiative "centralize command of cyberspace operations" is also repeated as part of the mission focus of USCYBERCOM which declared initial operational capability (IOC) on May 21, 2010.[2] While the context of both the QDR and USCYBERCOM's mission suggest a focus on defending Department of Defense (DoD) networks, they and the Commander of USCYBERCOM also discuss executing "full-spectrum cyber operations on command."[3] While other terms are used to further define the organization's responsibilities in cyberspace like "plan, integrate, coordinate, synchronize" it is obvious that the organization will, or is prepared to, exercise command (and control) of cyberspace operations in general. Given that fact, what are the implications for command and control of cyberspace operations? More specifically how should they be commanded and controlled? The mere standup of USCYBERCOM does not sufficiently address the latter question and neither will this paper. But, that is the point; it depends. However, addressing the initial question leads to the

[1] U.S. Department of Defense, *Quadrennial Defense Review* (Washington, DC: Secretary of Defense), 38.
[2] U.S. Strategic Command, "Fact Sheet, USCYBERCOM," http://www.stratcom.mil/factsheets/cc (accessed 28 September 2010).
[3] General Keith B. Alexander, Commander U.S. Cyber command (testimony, House Committee on Armed Services, Washington, DC, 23 September 2010).

primary implication that there is likely to be tension between a command organized around a domain with domain-focused objectives, and commands that are organized based on regional responsibilities and objectives, and are themselves engaged in operations in cyberspace.

The problem we are trying to avoid, other than the negative aspects of competing objectives, is the over-simplification or over-centralization of command and control for all cyberspace operations. The purpose of this paper is not to answer the question how should cyberspace operations be commanded and controlled, but to explore what effective command and control starting with command relationships should depend on. The short answer is that when it comes to command and control in the cyberspace domain (as in others) one size does not fit all. As with operations in other domains, the mission/objective is the dominant determinant, not the domain. Command relationships and command and control architectures should only be determined after a complete analysis of the specific mission is done. For cyberspace in particular the primary considerations are what and where. Cyberspace command and control should depend on what kind of cyberspace operation is being executed and where in the cyberspace domain it is being performed. Answers to those two questions (and the myriad of related questions) coupled with the primary objectives the operations support can and should lead to different command relationships and command and control schemes and military planners should account for this possibility.

In order to support this argument there has to be a common understanding of terms and their limitations. The natural next step is a better understanding of the cyberspace domain itself and a sample of the military challenges that result both from a defensive and offensive perspective. Those challenges will then inform the command and control discussion resulting in sample considerations to illuminate why flexibility should be retained

in determining command relationships and control decisions and how the objective should be used to inform those decisions. It is important first to come to grips with the true uses and limitations regarding labels and definitions.

On Domains & Definitions

In recent years there have been many different definitions for the term cyberspace within the defense community alone. The National Military Strategy for Cyberspace Operations (NMS-CO) defined it in 2006 as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."[4] The QDR used a different but in some ways similar definition in 2010. Both characterized it as a domain. The definition found in the QDR defines cyberspace as "a global domain within the information environment that encompasses the interdependent networks of information technology infrastructures, including the internet and telecommunication infrastructures."[5] The approved Joint definition uses similar language, but is additive: "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and imbedded processors and controllers."[6] Months or years could be wasted (and probably have been) arguing over whether or not cyberspace is a domain, whether the other aspects of the definition are accurate or complete, and/or which definition is better.[7] Pick the topic to be addressed (strategy, defense reviews, command and control, etc.) and the first issue is

[4] Chairman, U.S. Joint Chiefs of Staff, *National Military strategy for cyberspace Operations* (Washington, DC: CJCS, 2006), ix.
[5] U.S. Department of Defense, *Quadrennial Defense Review Report*, 37.
[6] Chairman, U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication (JP) 3-0 (Washington, DC: CJCS, 17 September 2006 Incorporating change 2, 22 March 2010), GL-12.
[7] The author was involved with the joint staffing while assigned to the Pentagon on the Air Force staff and has always considered the NMS-CO definition to be the most accurate and usable.

deciding on a definition of cyberspace. The directive nature of an approved joint term aside, this issue can be mitigated if not eliminated if the analyst, or military planner in the case of command and control, understands the limits and true impact of the term domain or any particular definition.

The term domain should simply focus the planner on core principles. It is a realization that like the other domains of air, land, sea, and space, military operations will take place in this domain. Like the other domains, friendly use or freedom of action will have to be defended, and adversary use or freedom of action may need to be denied. Additional analogies or conclusions should not necessarily be drawn nor should additional doctrinal tenets or operational concepts from other domains be automatically conferred upon it. Similarly, definitions should not be overused or over-relied on. While important, a definition is simply the first step in understanding the domain and usually purposefully concise. Its formulation or acceptance is not the end of thought or analysis, but the beginning. A fuller understanding of the domain and the implications to operations is required to inform any command and control decision.

Understanding the Cyberspace Domain and Military Challenge

Regardless of the definition stipulated, there are a few fundamental characteristics that are important regarding the cyberspace domain. First and foremost, unlike the other domains it is man-made. "It" was created for a purpose; actually a variety of purposes by a variety of people, groups, and organizations. It is a domain characterized by its man-made components (nodes) and the interconnectivity of those components. This leads to several other important characteristics: it exists within and across the other domains, it is a non-continuous domain, and it is volatile.

The very characteristics that intellectually and physically bound cyberspace (networks, the electromagnetic spectrum, infrastructures, etc.) allow it to exist across traditional domain boundaries. Individual nodes of cyberspace can exist on land, as well as in the form of satellites in space, airborne aircraft, and ships at sea. Although it can exist across traditional domain boundaries, cyberspace is by no means a continuous domain itself.

Although the cyberspace domain is becoming increasingly "interconnected," networks within cyberspace can be isolated. Adversary and friendly networks can be isolated both virtually and physically and still adhere to the above definitions. Networks can be isolated through techniques, such as protocols, firewalls, encryption, etc. or isolated by limiting either connectivity to other networks, and/or transmissions in free space. For example, many computer networks are isolated from the Internet simply because there are no physical connections to the Internet. Additionally, limiting communication in free space can isolate (to a degree) a network from intrusion, for example, by using buried fiber-optic cable as a communication means vice microwave, SATCOM, or other free space transmissions. The result is that the domain of cyberspace is actually a collection of domains or cyberspaces. In other words, cyberspace is made up of many different networks with many different functions, levels of interconnectivity, technical complexity, vulnerabilities, etc. (See Figure 1). Many of these networks are subject to volatility (in differing degrees) due to the high rate of technical innovation resident in the computer and communications industry.

Cyberspace in general is in a state of continual change. Specific networks within cyberspace will be responding to technical innovation; the addition, removal or replacement of components; software/firmware/protocol updates; not to mention entirely new networks being added. As the NMS-CO points out, "Cyberspace constantly changes, making some

targets transitory and offensive and defensive operations challenging. A previously vulnerable target may be replaced or provided with new defenses with no warning, rendering US offensive cyber operations less effective."[8] The reality of volatility and the other characteristics discussed points to the many military challenges of operating in the cyberspace domain; challenges that will and should impact command and control choices.

Though the characteristics of cyberspace enable the range of military operations, those characteristics also present many military challenges. The size and complexity of the domain and the extensive collection of networks within it present challenges both from a defensive and offensive standpoint that make ensuring and denying freedom of action in the domain difficult and sometimes elusive. Figure 1 depicts a generalized representation of the different networks that exist in the domain.[9]

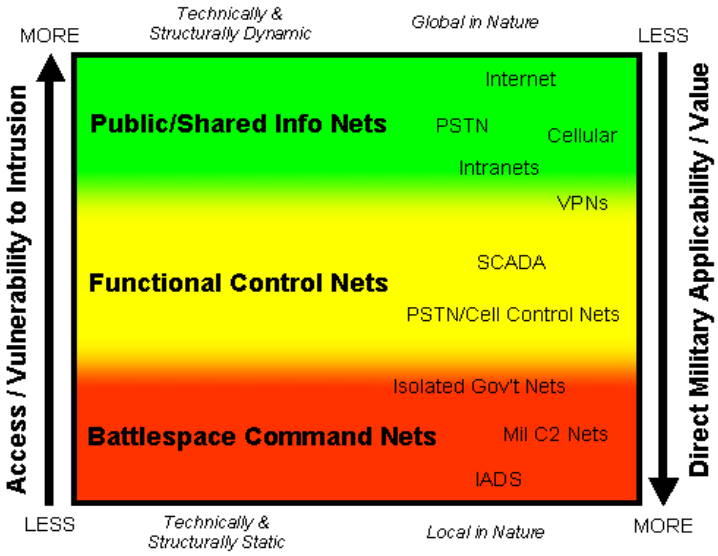

Figure 1. Representative Networks.

[8] Chairman, U.S. Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations*, 4.
[9] This figure was the combined work of multiple staff officers between USSTRATCOM and HQ USAF and used for illustrative purposes in multiple briefings in the 2006-2008 timeframe.

From a defensive standpoint, DoD must determine the level of connectivity necessary to both support distributed operations and information sharing, while still limiting vulnerabilities. In essence, the amount of connectivity is directly proportional to potential vulnerability. At the same time, the sheer number of geographically dispersed networks and nodes within the domain make it difficult for any one agency to defend the entire domain. The NMS-CO recognized this issue by stating, "DoD must ensure secure operation of its own portion of cyberspace and depend on other Federal Agencies to secure their portions of cyberspace." In fact, the responsibility for securing the nations critical cyber infrastructure was given to the Department of Homeland Security.[10] DoD for its part operates and must defend 15,000 different networks.[11] The importance of which was a driving factor behind the establishment of USCYBERCOM.[12]

The vastness and volatility of the domain arguably presents an even greater challenge to offensive operations. A premium is placed on true understanding of the individual characteristics of adversary networks and how they are used. Operations in and through these networks will differ. Different networks will have different vulnerabilities, employ different technology, have different legal and policy constraints, and have different levels of applicability to achieving overall objectives, etc. Usefulness of offensive capabilities is also directly related to one of the most important differences between networks: level of access.

Access to adversary networks is vital in determining courses of action with regard to networks. The most lucrative or important conventional military targets like enemy Integrated Air Defense Systems (IADS) are likely to be the most isolated and secure. This

[10] U.S. President, *The National Strategy for Securing Cyberspace*, (Washington, DC: White House, 2003, ix.
[11] U.S. Department of Defense, *Quadrennial Defense Review Report*, 37.
[12] William J. Lynn III, Deputy Secretary of Defense (address, USSTRATCOM Cyber Symposium, Omaha, NE, 26 May 2010.

suggests that while non-kinetic attack options may be preferable when possible, it is likely that a kinetic option or a combination of capabilities will be required to achieve a particular effect. While all networks have interconnectivity as a fundamental characteristic, they are not all interconnected to each other or globally. Access or vulnerabilities like free space links may only exits locally and require different capabilities to exploit. Conversely targeting adversary use of a relatively open network like the Internet, while also lucrative may be hindered by legal constraints and sheer redundancy of such a large network with many dispersed civilian nodes.

This suggests that countering adversary use (i.e. terrorist organizations) of the Internet, for example, is a significantly different problem than countering traditional military use of the cyberspace domain. Terrorist organizations themselves are dispersed social networks of individuals and groups. They utilize a public, commercial, highly interconnected, redundant, globally dispersed, regulated and unregulated, and sometimes anonymous domain, to recruit, communicate, educate, raise and transfer funds, etc. It poses a significant challenge for many reasons not the least of which is that you are trying to target a subset of a subset of cyberspace that may be continually changing and crossing traditional boundaries.

The point here is not to propose a solution to any of these problems, but to highlight the fact that they <u>are</u> different, just from the standpoint of the network in question. They are further differentiated by the operations being performed in or through the network(s). The term "cyberspace operations" does little to inform any problem. However, the definition provides a starting point. JP 1-02 defines cyberspace operations as: "the employment of cyber capabilities where the primary purpose is to achieve objectives in or through

cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[13] One more definition is required. Computer Network Operations is: "comprised of computer network attack, computer network defense and related computer network exploitation enabling operations."[14] It matters whether the task is to defend or attack the network and the network, its purpose and characteristics matter as well. If the networks that make up the domain are different, and the operations being conducted (defense or offense) are fundamentally different and focused on different networks, and the objectives being supported are different, then it stands to reason that effective command and control will be situation-dependant and not necessarily the same for all cyberspace operations.

On Command and Control

As mentioned up front, one of the problems we are trying to avoid is over-generalizing or pre-disposing command relationships or a command and control scheme for cyberspace operations. This is in response to the term having been introduced as part of the QDR initiative and excerpt from the USCYBERCOM focus of "centralize command of cyberspace operations." Having established that these operations can look very different depending on their nature (offensive or defensive) and that they are heavily dependent on the portion of cyberspace in question, it does not necessarily follow that command of all cyberspace operations should be centralized in one place. At the very least it is a matter of degree. What then should be considered in determining the best command and control relationship? What should be centralized and where?

[13] Chairman, U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02 (Washington, DC: CJCS, 12 April 2001 As amended through 31July 2010), 118.
[14] Ibid, 93.

This last question is crucial. Centralization is done for a variety of reasons, to ensure a common purpose, ensure efficient use of limited assets, to realize efficiencies in general, and many others. However, there is always something that is being centralized. Joint doctrine mentions centralizing overarching plans and enabling decentralized execution.[15] The United States Air Force has long held the tenant of centralized control decentralized execution which centralizes: "…planning, direction, prioritization, synchronization, and deconfliction of air and space capabilities…"[16] The QDR statement speaks of centralizing command which is centralizing a certain amount of control of particular forces. That control is being centralized at the sub-unified level (USCYBERCOM) of a functional Combatant Command (USSTRATCOM). Given this and the inherent tension between functional combatant commands and the additional tension provided by the vastness of the cyberspace domain, the command and control discussion here will focus on command relationships that include levels of control. Specifically, the command relationships necessary to execute the broad missions of network defense and network attack and employ the forces required.

Much like the term "cyberspace operations" required clarification, so too does the phrase "centralize command" regardless of the context. This is true even if the list of what is being centralized appears to be specific (like that of Air Force doctrine). This is based on the fact that command and control is not just about lists of tasks or functions and who is doing them, it is essentially decision-making or a series of decisions. Even with the concept of centralized control/decentralized execution, the difference between where control ends and execution begins is an imaginary line between what decisions are made and where. As there

[15] Chairman, U.S. Joint Chiefs of Staff, *Doctrine for the Armed forces of the United States*, Joint Publication (JP) 1 (Washington, DC: CJCS, 2 May 2007 Incorporating change 1, 20 March 2009), IV-15.
[16] U.S. Air Force, *Air Force Basic Doctrine*, Air Force Doctrine Document (AFDD) 1 (Washington, DC: Department of the Air Force, 17 November 2003), 28.

is a chain of command, there is more of a continuum of control. Decisions are being made regarding the employment of forces from the Combatant Commander all the way to the unit in the field, where every decision assumes a certain amount of control. While that includes a multitude of decisions, the continuum begins with broad decision-making authority at the combatant command level of COCOM, OPCON, and TACON. Those terms are generally defined in figure 2 below in relation to when they should be delegated.[17]

Figure 2. Command Relationships, from Joint Publication 1.

The tension arises when one combatant commander requires forces (or authorities) that are assigned to another combatant commander. While COCOM authority cannot be transferred, OPCON and TACON can. The decision to transfer that control is like everything else, situation dependent, therefore with regard to this discussion there will be no definitive case made for or against transferring control. Rather, the goal is to put forth considerations

[17] Chairman, U.S. Joint Chiefs of Staff, *Doctrine for the Armed forces of the United States*, Joint Publication (JP) 1 (Washington, DC: CJCS, 2 May 2007 Incorporating change 1, 20 March 2009), IV-2.

to inform that decision which will depend on numerous factors that will differ in each case. First, regardless of the planning process or approach, command and control discussions should happen only after a thorough analysis of the environment and the problem, and always informed by the objective at every level. Even if initial supported/supporting relationships are anticipated, flexibility should be retained in determining command relationships for particular forces. Given the differences already discussed between network defense and network attack, and the different networks in cyberspace, these choices should not be made until a complete network analysis has been done as part or in support of mission analysis. The results are likely to be different in terms of the different operations, as are the considerations.

Considerations for both defense and attack should begin with the mission and objective being supported. A sample of some important considerations (in the form of questions) is contained in the figure below. Again, while not necessarily advocating a serial approach, clearly specifying the network and its purpose is an important step. Of course a thorough network analysis will address many of these questions and lead to many more. But, with regard to command and control and command relationships it is important to get to the questions of: what decisions need to be made and who is in the best position to, and/or should make each of these decisions? It may not be the same person or

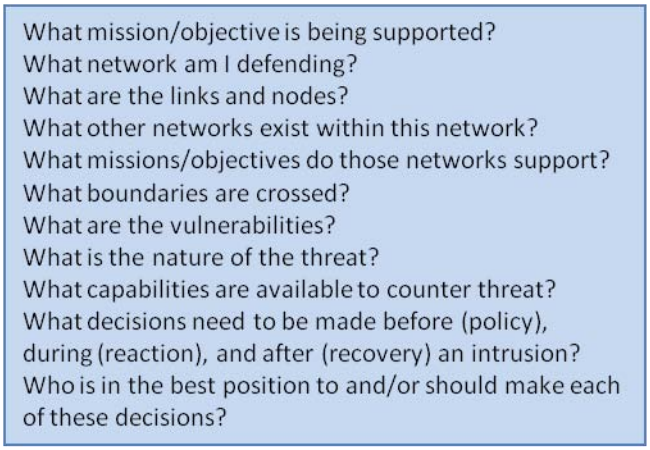

Figure 3. Defensive Considerations

organization in all instances. This is especially true if employing a defense in depth strategy with regard to a large worldwide network like DoD's Global Information Grid (GIG) that crosses many regional command boundaries. Since every node is a potential vulnerability that could affect the rest of the network, it makes sense to centralize many policy, reaction, and recovery decisions. However, it would also be necessary to delineate what level of autonomy is required along the depth of the defense. There are many important reasons for this not the least of which is preserving an ability to react quickly to an intrusion.[18] Similar considerations are useful from a network attack perspective as well.

Obviously the mission and objective being supported is just as important from an offensive standpoint. The network of course is going to be different from situation to situation, perhaps even from objective to objective. An adversary could be utilizing many different networks to support their operations (command networks, IADS, internet, cell, etc.). All networks support a purpose (man-made), therefore it is important to understand the social network the physical network is supporting.

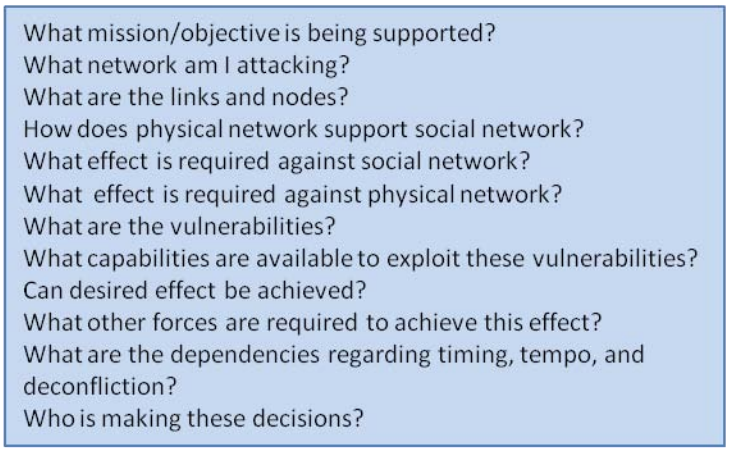

Figure 4. Offensive Considerations

Significantly, there may be situations where the social network is the overriding consideration (i.e. an ill-structured problem). Just because you have the ability to effect the

[18] Of course these decision points and choices should be looked at holistically. Good policy and procedures put in place before hand could also aid in shortening response time.

physical network doesn't mean you should.[19] Additionally, the ability to achieve a particular effect on a network may require the synchronized and deconflicted employment of multiple capabilities. Again, network analysis in conjunction with mission analysis will lead to an understanding of the decisions that need to be made and who should be making these decisions. The capabilities required is an important consideration, but who owns them (COCOM) is of secondary importance unless they are unavailable for tasking. The primary consideration again for both defense and attack is the mission or objective being supported.[20]

Given the primacy of the objective it makes sense that this should be the most important consideration when determining command relationships and control of forces. In this regard the idea of "coupling" found in Marine Corps Doctrinal Publication (MCDP) 5 for planning is useful in informing these decisions. MCDP 5 describes plans as tightly or loosely coupled and defines coupling as "a relative term referring to how closely two or more actions in a plan interact…" where tight coupling "…means there is a close relationship between two parts."[21] In this regard, during mission analysis before command relationships or command and control choices are made, planners should look at how tightly coupled the cyberspace operations of defense and attack are to the objective and who or what organization is primarily responsible for that objective.

From a defensive standpoint USCYBERCOM through USSTRATCOM has been assigned the mission of defending the GIG.[22] Numerous actions around the globe taken in

[19] This is not to say that the effect on people supporting an IADS in a more structured conventional problem is not important, but to stress the importance of the type of overall problem being faced and the consequences of action.
[20] Neither list of considerations is meant to be all-inclusive. They are simply illustrative of questions that should be asked in order to understand the network and get to important decision points. There are many more.
[21] U.S. Marine Corps, *Planning*, Marine Corps Doctrinal Publication (MCDP) 5 (Washington, DC: HQ U.S. Marine Corps, 1997), 50.
[22] Department of Defense, *Unified Command Plan* (Washington DC: Office of the Secretary of Defense, October 2008).

the numerous networks that make up the GIG could be said to be tightly coupled with this mission/objective. It makes sense then to centralize significant authority and control of certain/any defensive forces with USCYBERCOM. This should be done while ensuring that others who are relying on these networks are still able to accomplish their mission. Actions and risks to the overall network must be balanced with the objectives of those using a certain portion of it. In this sense some decisions or autonomy may be decentralized based on the fact that sub-networks may be loosely coupled physically or logically with the GIG and that there will always be some local responsibility to defend "your network." Attacking adversary networks will be different, but can be looked at the same way.

Geographic and Functional Combatant Commanders have multiple assigned and implied missions worldwide. Many have the requirement to deny adversaries or potential adversaries use of different portions of cyberspace. It stands to reason that if a network is being attacked in support of a regional objective it is obviously coupled to that objective. Adding to this coupling is a likely requirement for any attack through cyberspace to be synchronized and deconflicted with other capabilities also affecting that network and other related but separate operations. Coupling to the social network is also an important consideration. The ability to monitor effects on a local social network again more tightly couples the action to the regional command or local commanders. Tighter coupling makes a stronger case for more authority and control of attack capabilities by the organization responsible for that objective (i.e. a geographic combatant command). Loosely coupled network attack actions may be satisfied with simple support relationships. More tightly coupled actions may require transfer of at least TACON. USCYBERCOM is likely to

support, however control of any forces (fires, timing, and tempo) will be transferred to the regional commander.

Summary

What is left then is not an answer for every situation or any situation, but questions. What and where? Command relationships and control of forces in cyberspace depends on what cyberspace operation is being performed and where in the cyberspace domain (network) it is being performed. Since command and control is essentially decision-making and the authority to make decisions it depends on what objective or mission is being supported, what decisions need to be made, and who (where) should make those decisions. The objective being supported will determine what is centralized and where. Cyberspace command and control itself is a misnomer. The military does not command and control domains it commands and controls forces. It uses those forces to exert control over others operating in that domain. General terms like cyberspace, cyberspace operations, and centralize command do little to inform choices. It depends on a much deeper understanding of the environment and the particular problem being addressed. It depends.

Counterargument

There is no true counterargument out there that suggests that it does not depend, and it would not be useful if there was. The primary counterargument revolves around an approach for cyberspace command and control centered on USCYBERCOM and then varying sub-arguments regarding degrees of control usually employing supporting relationships and coordination instead of transferring TACON or OPCON. The military challenges, some of which were discussed in this study, are used to justify centralization as it pertains to cyberspace or cyberspace operations. Focusing the limited cyberspace expertise

at USCYBERCOM allows CDR USCYBERCOM to execute cyberspace priorities and support the spectrum of military operations. Due to limited forces, TACON or OPCON cannot be transferred due to the potential need to support elsewhere so it is more appropriate to set up supporting relationships as outlined in JP 1, where timing and tempo ostensibly would still be dictated (requested) by a regional or other commander and potentially supported by a coordinating authority.[23] Unfortunately many of the arguments use generic potential scenarios or single issues to rule out transferring control, but do not allow for or discuss the potential scenarios where it may be appropriate. They also fail to fully address the fact that the Secretary of Defense adjudicates priorities between combatant commands when necessary. Finally, a universal structure may be appropriate for certain situations and may have merits regarding replication and simplicity in planning and setting up that structure habitually. However, maintaining the intellectual and military flexibility to utilize all options available in solving what are likely to be very different problems in today's environment seems like the better choice.[24]

Conclusions/Recommendations

That is the primary conclusion and recommendation: do not implement a universal command and control architecture for "cyberspace operations" centered on USCYBERCOM or any other command. Given that, the overall recommendation to anyone involved in determining command relationships and control architectures is to do the analysis. Do not leave it to someone else or expect the General or Flag Officers to "figure it out." The

[23] David M. Franklin, "U.S. Command Relationships in the Conduct of Cyber Warfare: Establishment, Exercise, and Institutionalization of Cyber Coordinating Authority," (Newport, RI: Naval War College, 3 May 2010). Many of these arguments are alluded to in Franklin's paper. However, I cannot do his argument justice in the limited space. What is here is a conglomeration of a general counterargument, many of the concepts the author has seen applied to certain space forces in his own experience.

[24] The transference of operational and tactical control is of course a regular and habitual occurrence for other forces and has been for a long time.

analysis will take time and recommendations to those officers should be based on that thorough analysis. It should not be an afterthought of course of action selection or planning in general, or a matter of dusting off an old architecture, unless it fits the analysis. Short-cutting the analysis regarding the key decision points and who should make them may be a time saver early on, but it could potentially lead to larger problems and mission failure down the road.

In order to better inform the analysis, any guidance, doctrine, orders, and statements should avoid using the term cyberspace or cyberspace operations. We command and control forces, to accomplish tasks, in support of missions, to achieve objectives. Discussion of operations should use the specific task or mission such as "computer network attack." When possible include the network in question like "defense of the GIG." Additionally, the discussion here focused simply on network defense and network attack operations. Additional tasks or concepts like operating the network, network exploitation, or active defense should be given the same scrutiny and not confused with other operations.[25]

In closing, USCYBERCOM has a very important mission focused on a very important domain. That domain, however, is vast and complex with many operations being done in, through, and certainly supported by it. As with the term domain itself, the core principles of command and control apply to cyberspace operations, but the approach should not be over-simplified. The analysis is vital. The results of that analysis will be different from task to task, mission to mission, situation to situation. Some similarities may exist from time to time, but the "what" and "where" matter every time.

[25] William J. Lynn III, Deputy Secretary of Defense (address, USSTRATCOM Cyber Symposium, Omaha, NE, 26 May 2010). Secretary Lynn discussed active defense in particular as part of an overall defense strategy and response to a threat.

BIBLIOGRAPHY

Alexander, Gen Keith B., Commander, U.S. Cyber Command. Testimony. House Armed Services Committee on U.S. Cyber Command: Organizing for Cyberspace Operations, Washington D.C. 23 September 2010. http://armedservices.house.gov/pdfs/FC092310/AlexanderStatement.pdf (Accessed 16 October 2010)

Franklin, David M. "U.S. Command Relationships in the Conduct of Cyber Warfare: Establishment, Exercise, and Institution of Cyber Coordinating Authority." Newport, RI: Naval War College, 3 May 2010.

Lynn, William J. III, Deputy Secretary of Defense. Address. USSTRATCOM Cyber Symposium, Omaha, NE, 26 May 2010. http//www.defense.gov/speeches/speech.aspx?speechid=1477 (accessed 18 October 2010)

Scherrer, Joseph H. and William C. Grund., *A Cyberspace Command and Control Model*, Air War College Maxwell Paper. No.47. Maxwell, AFB AL: Air University Press, August 2009.

U.S. Air Force. *Air Force Basic Doctrine*. Air Force Doctrine Document (AFDD) 1. Washington, DC: Department of the Air Force, 17 November 2003.

_____. *Cyberspace Operations*. Air Force Doctrine Document (AFDD) 3-12. Washington, DC: Department of the Air Force, 15 July 2010.

U.S. Department of Defense. *Quadrennial Defense Review Report*. Washington DC: Office of the Secretary of Defense, February 2010.

_____. *Unified Command Plan*. Washington DC: Office of the Secretary of Defense, October 2008.

U.S. Marine Corps. *Planning*, Marine Corps Doctrinal Publication (MCDP) 5. Washington, DC: Headquarters U.S. Marine Corps, 1997.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02. Washington, DC: CJCS, 12 April 2001 As amended through 31 July 2010.

_____. *Doctrine for the Armed Forces of the United States*, Joint Publication (JP) 1. Washington, DC: CJCS, 2 May 2007 Incorporating Change 1 20 March 2009.

_____. *Information Operations*, Joint Publication (JP) 3-14. Washington, DC: CJCS, 6 January 2009.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Operations*, Joint Publication (JP) 3-0. Washington, DC: CJCS, 17 September 2006 Incorporating Change 2, 22 March 2010.

_____. *Joint Operation Planning*, Joint Publication (JP) 5-0. Washington, DC: CJCS, 26 December 2009.

_____. *The National Military Strategy for Cyberspace Operations*. Washington, DC: CJCS, December 2006. Document is now declassified.

U.S. President. *The National Strategy to Secure Cyberspace*. Washington, DC: White House, 2003.

U.S. Strategic Command, "Fact Sheet, U.S. Cyber Command," http://www,stratcom.mil/factsheets/cc/ (accessed 28 September 2010).