REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

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

4. TITLE AND SUBTITLE

Planning for Cyberspace: Ensuring the Integration of Cyberspace Into the Joint Operations Planning Process at the Geographic Combatant Command

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lt Col Shawn N. Bratton, ANG

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 advent of cyberspace as a warfighting domain has brought increased attention and an even greater amount of discussion regarding how best to plan and conduct operations in this arena. Planning staffs are each Geographic Combatant Command are routinely planning operations in the air, land and sea domains. Some action must be taken to ensure that the Geographic Combatant Commander have the appropriate planning resources available to conduct deliberate and crisis action planning and ensure that cyber capabilities and the cyber domain are synchronized and integrated with more conventional effects . Cyber planners must be embedded at the Geographic Combatant Command in order to ensure cyber capabilities and considerations are fully integrated into the Joint Operational Planning Process.

15. SUBJECT TERMS

Cyberspace, cyber planning, JOPP

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		21	19b. TELEPHONE NUMBER *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

Planning for Cyberspace: Ensuring the Integration of Cyberspace into the Joint Operations Planning Process at the Geographic Combatant Command

by

Shawn N. Bratton

Lt Col, Air National Guard

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

Abstract

The advent of cyberspace as a warfighting domain has brought increased attention and an even greater amount of discussion regarding how best to plan and conduct operations in this arena. The Department of Defense has taken note of these activities and created United States Cyber Command to plan and conduct cyber related actions. However, the enemies fighting in cyberspace physically reside in the areas of responsibility (AOR) of a Geographic Combatant Commander and the planning to combat these enemies takes place in, and is the responsibility of, the planning staff assigned to each Geographic Combatant Command. Combatant Commander's have the responsibility to plan and execute operations against the enemies who physically operate and reside within their respective AORs. Planning staffs at each Geographic Combatant Command are routinely planning operations in the air, land and sea domains. Some action must be taken to ensure that the Geographic Combatant Commander have the appropriate planning resources available to conduct deliberate and crisis action planning and make certain that cyber capabilities are synchronized and integrated with more conventional effects. Cyber planners must be embedded at the Geographic Combatant Command in order to ensure cyber capabilities and considerations are fully integrated into the Joint Operational Planning Process.

Introduction

In both Iraq and Afghanistan, a variety of non-kinetic systems have served as force multipliers; however, their full operational potential has not been realized because of the fragmented manner in which they are applied to the fight.

- Brigadier General Michael J. Cary, Deputy Director, Global Operations, U.S. Strategic Command

The advent of cyberspace as the newest warfighting domain has brought a great deal of attention and an even greater amount of discussion on to how best plan and execute operations in this arena. Each of the military services has developed a component dedicated to presenting capabilities in cyberspace.[1] Planning staffs around the world that have traditionally practiced their operational art in the arenas of air, land and sea are now working to understand and include cyberspace. While there had been the previous discussion on integrating new domains as the space domain became more recognized and relevant, the space domain ultimately had little impact on a traditional planning staff since the Geographic Combatant Commander's area of responsibility (AOR) does not include the physical overhead space domain and their plans already accounted for the supporting space infrastructure that existed on the land.[2] The introduction of the cyber domain presents a significantly different set of challenges. Unlike space, potential enemies have already made significant advances in this domain that include offensive actions. Additionally, both state and non-state actors have demonstrated a willingness to operate in cyberspace, conducting

[1] Each of the services has a cyber component which in turn supports USCYBERCOM. Service Elements include Army Forces Cyber Command (ARFORCYBER); 24th USAF; Fleet Cyber Command (FLTCYBERCOM); and Marine Forces Cyber Command (MARFORCYBER).
[2] Annex N of an OPLAN contain information and considerations for the space domain

information operations which have in turn produced significant results for our enemies.[3] The Department of Defense took note of these activities and in 2009 Secretary Gates directed United States Strategic Command to stand up a new sub-unified command to focus on this domain; United States Cyber Command (USCYBERCOM) was born.[4] USCYBERCOM's mission is to, "plan, coordinate, integrate, synchronize, and conduct activities to direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."[5] However, the enemies fighting in cyberspace physically reside in the AORs of the Geographic Combatant Commanders and the planning to combat these enemies takes place in, and is the responsibility of, the planning staff assigned to each Geographic Combatant Command. This creates an immediate disconnect as USCYBERCOM stands up with the expertise to handle warfighting in this domain, and yet it is the Geographic Combatant Commander who will have the responsibility to plan and execute full-spectrum operations against the enemies who physically operate and reside within their respective AORs.[6] Some action must be taken to ensure that the Geographic Combatant Commander has the appropriate planning resources available to conduct deliberate and crisis action planning. Cyber planners must be embedded at the Geographic

[3] The New York Times detailed use of computer network attacks against Georgia by state sponsored groups during the 2008 conflict (Markoff, *Before the Gunfire, Cyberattacks)*.
[4] The SECDEF memo entitled *Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations* outlines organizational changes, timeline requirements and the initial command and control structure for USCYBERCOM.
[5] Department of Defense fact sheet on USCYBERCOM.
[6] It is the Geographic COCOMs that are tasked with developing theater security cooperation plans and specific Concept Plans and Operation Plans for the countries in their assigned Area of Responsibility. Each command has a planning staff that conducts planning activities to develop these products. These plans should account for the cyberspace domain as well as every other domain and the joint planning process ultimately provides the commander with integrated options for a successful operation.

Combatant Command in order to ensure cyber capabilities and considerations are fully integrated into the Joint Operational Planning Process.

Planning for Cyberspace

Before addressing the planning functions and staffs that lay at the crux of the discussion it is important to define the terms and help ensure a common understanding of the issue. When speaking of cyberspace this is particularly important as so many aspects are still undefined or are defined differently by the services. As a foundation, Merriam-Webster defines cyberspace as, "the online world of computer networks and especially the internet."[7] The Department of Defense's joint publications elaborate further and define cyberspace as "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[8] At times cyberspace is referred to as a capability, usually in concert with discussing a "cyber attack" and other times it refers to the domain through which information flows.[9] Throughout this paper the term cyberspace will refer to the domain as defined by the joint publication and the term Computer Network Operations will be used to refer to operations that occur within the cyberspace domain. Computer Network Operations can itself be subdivided into components, such as computer network defense or computer

[7] Merriam-Webster online dictionary.
[8] JP 1-02, p 118.
[9] Dan Kuehl from National Defense University discusses cyber as a synonym for Computer Network Operations and uses the term connectivity to describe the portion of the information environment across which content flows and thoughts (cognition) can be generated. In this language connectivity is the equivalent to the DoD's definition of cyberspace.

network attack; however, this paper will use the umbrella construct of Computer Network Operations and specify the sub-components only when differentiation is warranted.[10]

In addition to defining terms it is also appropriate to briefly address the scope of this paper. At its heart this paper is about the planning staff and the actions taken by that staff on behalf of the combatant commander. It is not a paper about command and control. As arguments are made for placement of planners at the Geographic Combatant Command, it is not the intent to state to whom these planners should be assigned, nor is there a position on Operational Control (OPCON) or Tactical Control (TACON) of operational units. Command relationships for operations are built during the planning process and should be the result of careful consideration by the planning staffs in light of the mission requirements and associated circumstances.[11] While this paper does advocate for physically placing planners at the Geographic Combatant Command it is not stating the planners should be assigned to a regional commander. This will be discussed further in the recommendations. This paper will not address intelligence support to cyber operations, and it will not address the orders development stage of the JOPP. Instead it will focus on how to best integrate the planning of cyber operations within the JOPP with an emphasis on mission analysis and course of action (COA) development. Finally, this paper will not address a cyber only scenario. While single domain response options have been employed (an air strike for example) it seems unlikely that a COCOM's OPLAN will be developed with the only option being a single domain COA. Finally this paper assumes the reader has some familiarity with the Joint Operations

[10] Computer Network Operations divides into four subcomponents: Computer Network Attack, Computer Network Defense, Computer Network Exploitation and Network Operations.
[11] C2 relationships are defined throughout planning and at all levels. The SECEF will designate supporting and supported commanders as well as assign forces to a Combatant Commander. Higher level commanders will define the appropriate command relationships for the subordinates. Commanders will outline additional authorities as appropriate to execute a given task or plan.

Planning Process and will not attempt to educate on the specific steps but rather show the implications of cyberspace planning in the steps addressed.

The Importance of Integration and Synchronization

The Joint Operational Planning Process exists to provide "a methodical approach to planning at any organizational level and at any point before and during joint operations."[12] Like air, land and sea forces, cyber forces will be employed as part of a joint force and may have effects that carry across the other domains. Each service will develop and mature their own capabilities to operate in the cyber domain and present these forces to the joint commander for employment. A joint planning group that is formed by a joint force commander to conduct planning will usually be comprised of staff representatives, component representatives and other supporting organizations and this planning staff will determine how best to employ the forces provided in an integrated and synchronized manner to ensure unity of effort.[13]

Integration, as defined by Joint Publication 1-02 is, "the arrangement of military forces and their actions to create a force that operates by engaging as a whole."[14] Integration brings together individual forces components such as tanks, planes, soldiers and artillery and employs them as a single force. Doctrine and experience point to the need for the integration of capabilities and require the joint force commander to employ forces to ensure integration and subsequently, unity of effort. Milan Vego states, "Unity of effort is one of the main prerequisites of successful performance at any level of command."[15] This seems intuitive, but it is important to examine why warfare is conducted in this manner, acknowledge that

[12] JP 5, p I-11.
[13] JP 1-02, p 254.
[14] JP 1-02, p 230.
[15] Vego, p VIII-13.

Computer Network Operations must be integrated just as other forces are integrated, and consider the impact this concept has on planning. In the case of a planning staff unity of effort is just as critical as it is for the forces in execution as it helps ensure success during the Joint Operations Planning Process.

The term synchronization is often used to refer to the integration and alignment of capabilities in time. Joint publications define synchronization as, "The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time."[16] Computer Network Operations effects must be synchronized with conventional effects in support of the joint commander's objectives. If USCYBERCOM conducts the operational planning for Computer Network Operations, it introduces risk that this separate plan will not be completely synchronized with the conventional effects provided by the Geographic Combatant Command. The reason for this is that synchronization, by definition, requires an understanding of the time, space and force factors that are generated, discussed and defined by the planning staff at the Geographic Combatant Command. Should USCYBERCOM proceed with their own development of time, space and force factor considerations they will certainly be different than those generated by the Geographic Combatant Command planning staff. If the factors are forwarded to USCYBERCOM for use in planning then there will not be the depth of understanding of these functions that is required to put them to use throughout the rest of the planning process. While consideration in planning for conventional effects does require significant inputs from outside sources such as the supporting functional component commanders, these commanders are part of the same Joint Task Force or Unified Command whereas USCYBERCOM is not, rather USCYBERCOM will be serving as a supporting

[16] JP1-02, page 453.

command to the Geographic Combatant Commander. Ultimately this presents difficulties in conducting separate planning efforts for cyberspace that do not exist with other domains due to their representation by a subordinate functional command.[17]

Exercise TERMINAL FURY 2010 addressed this by including a Joint Cyber Operations Task Force that was a forward operating element from USCYBERCOM but not a subordinate command to PACOM.[18] These planners were certainly able to assist in the synchronization efforts, however, because their arrival was after the OPLAN development stages of the exercise their effectiveness was more geared to execution rather than planning.[19] Operational factors that are common to the PACOM planning staff were new to the JCOTF and specific cyberspace factors were likely new to the PACOM planning staff. In order to achieve integration and subsequently the unity of command and synchronization required for successful employment of a force, an operational plan must be built with a common understanding of the factors determined in the Joint Operations Planning Process.

Cyberspace in the JOPP

> *War plans cover every aspect of a war, and weave them all into a single operation that must have a single, ultimate objective in which all particular aims are reconciled.* – Clausewitz, *On War*

The Joint Operation Planning Process provides a planning framework that can be used to generate Operations Orders (OPORDs) and Operation Plans (OPLANs). The JOPP is broken into steps and is intended to guide that staff through an orderly process to analyze a

[17] There has been no significant discussions about making a Joint Cyber Component Commander on par with the JFACC, JFLCC, etc. Rather each component commander employs capabilities in the cyber domain, usually along service lines.
[18] TERMINAL FURY is a PACOM hosted command post exercise conducted annually to prepare PACOM to confront challenge in its assigned AOR.
[19] There are several references to the Joint Cyber Operations Task Force. In his 23 Sept 2010 Congressional testimony, General Alexander discussed the JCOTF as a task force that will go forward to work with a Geographic Combatant Commander. The JCOTF participated most significantly in phase II (execution phase) of the TERMINAL FURY command post exercise.

situation and the appropriate guidance, develop courses of action for the commander and ultimately generate a plan or order. At each step of the process the planning staff will complete actions and prepare recommendations within their functional areas of expertise.[20]

Mission Analysis

Mission analysis is focused on gaining a better understanding of the task at hand, or as the joint publication states, "The primary purpose of mission analysis is to understand the problem and purposes of the operation and issue appropriate guidance to drive the rest of the planning process."[21] During mission analysis planners must identify facts and assumptions, make determinations regarding specified and implied tasks, and clearly define restraints and constraints. These considerations form the basis for the planning effort and inform every subsequent step of the JOPP.

As planners meet to conduct the initial mission analysis, discussions occur on the intent of higher headquarters, the scope of the mission, and the forces available. The Joint Intel Preparation of the Operating Environment (JIPOE) that is developed must include aspects of the cyber domain in order to ensure appropriate consideration as planning moves forward. These initial discussions by the planners will form the intellectual framework for the rest of the planning process and are critical to developing an understanding of the intent of the commander. These discussions also serve the purpose of bringing the planning staff together as a team. As the staff begins to develop a deeper understanding of the problem late arrivals may not be able to catch up and their intellectual foundation will be weak. From this point on additional planners arriving to contribute or attending via other mean (video teleconferencing for example) are likely to be seen as outsiders, particularly if there is not a

[20] JP 5, page III-3.
[21] JP 5, p III-21.

face-to-face contact. While their contributions may be valuable and incorporated, they are more likely to be discounted.[22]

Planning staffs are generally comprised of personnel with a variety of backgrounds from each of the services. Due to the newness of Computer Network Operations and the paucity of military units that operate within the cyber domain it is unlikely that a military member on a planning staff will have experience in cyberspace.[23] Currently planning staffs intend to rely on USCYBERCOM for this expertise, as was the case for TERMINAL FURY. However it is unlikely that outside USCYBERCOM planners will be involved in the early stages of mission analysis. Inclusion of USCYBERCOM is more likely to occur once available forces are analyzed later in the mission analysis phase. Involvement is even less likely if the planning effort is directed by the local commander vice something directed out of the Unified Command Plan where USCYBERCOM would be formally tasked as a supporting command. Additionally, it is not realistic to expect that USCYBERCOM can respond and participate in every Joint Planning Group that comes along as these are frequent and vary in scope.[24] However, it is important that even at the early stages of mission analysis, a cyber expert is involved to ensure that the proper implied tasks, restraints, assumptions and priority intelligence requirements (PIRs) are developed in support of the planning efforts. These are the things that will lay the groundwork for integration and rapidly shape COA development.

---

[22] Khosrow-Pour, p 36 examines the value of fact-to-face meeting vice conducting business over other means.
[23] During his testimony before the House Armed Services Committee, General Chilton, CDR USSTRATCOM, discusses the challenge of getting the right experience into the right position.
[24] In the author's experience at the JACCE in Iraq, MNF-I and MNC-I were routinely running multiple planning groups at any given time. Likewise at JFCC-SPACE/14th Air Force, JPGs were frequently stood up to address a variety of issues.

As staffs begin to develop an understanding of the operational time, space and force factors they must consider the cyber domain and understand how cyberspace may or may not impact the traditional domains of air, sea, land and space. For example, as the planning staff develops an understanding of an enemy's command and control mechanisms, the cyber domain becomes a key factor in time and space if the enemy is using the internet to coordinated activities. This may allow the enemy to coordinate the use of force in the land domain and direct movement of their forces at sea.[25] This command and control ability may in turn be identified as a critical vulnerability during further analysis. This discussion becomes foundational to developing the areas of interest, centers of gravity and will go on to shape course of action development. As with the earlier discussions on factors and functions, the integral nature of these discussions requires the cyber planner to be in the room. As mission analysis continues through development of the Commander's Critical Information Requirements (CCIRs) and PIRs, Computer Network Operations must be considered alongside conventional capabilities, particularly in the development of priorities for intelligence. An embedded cyber expert will not only ensure that these products appropriately include CNO language, but that planner will ensure the commander's authority and priority is appropriately assigned. Ultimately inclusion of the cyber planner in the process as part of the planning team is critical as it is the mission analysis process that will inform the next stage of the JOPP, Course of Action (COA) Development.

[25] Crowell's discussion the enemy's use of cyber networks in information warfare, expanding on Kuehl's thoughts of connectivity and cognition, is another example of how time, space and force must be considered with regard to the cyberspace domain. In that case the enemy was able to rapidly developed and disseminated influence products through cyber networks (rapid access to the world). Crowell, *Slaughtered Sheep*, p 14.

Course of Action Development

As a planning team begins to generate COAs for the commander to consider is it important that a cyberspace planner be present as an active member of the planning team. The brainstorming phase of COA Development is designed to generate options that may prove to be viable COAs. During this period a staff must make initial evaluations on the feasibility of a COA. Determinations made on a cyber specific COA or a COA that contains cyber actions will need some level of expertise in order to make an initial feasibility determination. While there is a general understanding throughout military members on a planning staff regarding the implications of putting "boots on the ground" or conducting a kinetic strike with aircraft, it is unlikely that there will be the same level of understanding with regard to cyberspace and Computer Network Operations activities. Specific Intelligence, Surveillance and Reconnaissance (ISR) requirements based on an understanding of the environment and enemy capabilities as well as the potential to use cyber capabilities as a non-lethal operational fire become import considerations for COA development. Interjecting these suggestions without an understanding of the operational environment and the enemy's capability introduces risk for the commander.

It is equally important to USCYBERCOM that a developed COA that can be executed in support of the Geographic Combatant Commander. Cyber expertise at this initial COA development stage will reduce the eventual workload on supporting cyber organizations as the cyber planner will credibly check the COA for feasibility and completeness. Additionally, a cyber planner will be able to better explain both to the Geographic Combatant Commander and to USCYBERCOM the intentions and rationale that went into the development of the COA should it later be selected. The embedded planner

will have the benefit and credibility associated with being part of the planning team and will be able to better explain the rationale and intent of a specific course of action.

COA Analysis and Wargaming

Just as mission analysis and COA Development require expertise in the AOR, the enemy, and the cyber domain, it is important to have the same experience available for COA Analysis and Wargaming. While outside players may be able to provide some value in the feasibility of a specific COA, a cyber planner with an understanding of the specific theater and operating area will provide significant inputs regarding the likely enemy actions and reactions. Just as experts in the maritime domain will speak to the impact of their actions on the enemy's navy and present likely counter-actions, an expert in the cyber domain will provide legitimate feedback to planners on actions and reactions that will challenge the planning staff to think critically about red team inputs. In this case it is the integration of cyber into enemy responses that becomes the critical requirement and drives the need for a cyber planner during wargaming and the subsequent COA Analysis.

Conclusions and Recommendations

In preparing for battle I have always found that plans are useless, but planning is indispensable – Dwight D. Eisenhower

Ultimately the result of the Joint Operations Planning Process is a joint operations plan or order. In response to the circumstances presented the plan will provide integrated and synchronized effects across multiple domains in order to achieve the joint commander's objectives. The makeup of the planning team is critical to ensure the development of the plan. Due to the new nature of cyber as a domain, specific planners must be sought out and brought to the planning staff in order to integrate capabilities across this domain. These

planners must have knowledge of both the cyber domain as well as an understanding of the AOR, the enemy and the current situation.

USCYBERCOM has just as much to gain as the Geographic Combatant Commander from embedded planners who will be better able to support synchronization of cyber effects due to the enhanced understanding of the situation. Additionally, embedded planners will be able to suggest employment of cyber effects at specific points along the timeline as the planning staff begins to pull together a timeline and synchronization matrix. Essentially rather than USCYBERCOM waiting for planners to pull information from them, an embedded planner will be better able to suggest inclusion of cyber as a push action (proactive rather than reactive). Ultimately, to be effective in a JPG an embedded cyber planner must have an understanding of the operational environment and the enemy as well as have expertise in the cyber domain. In order to achieve this a cyber planner must be a permanent fixture on the planning staff at each Geographic Combatant Command. Whether or not this planner is assigned and works for the Geographic Combatant Commander or is attached a permanent liaison officer is immaterial. The bottom line is that the cyber planner must be permanent party at the Geographic Combatant Command.

Counter Argument

The commander of USSTRATCOM is also responsible for synchronizing planning for cyberspace operations, planning against cyberspace threats, coordinating with other combatant commands and appropriate US government agencies prior to the generation of cyberspace effects that cross areas of responsibility, and executing cyberspace operations, as directed.

- Brigadier General Michael J. Cary, Deputy Director, Global Operations, US Strategic Command

A lack of cyber expertise outside of USCYBERCOM, a specific tasking to conduct planning, and ultimately ownership of a limited amount of CNO operational assets are reasons USCYBERCOM can put forth in defense of their ownership of the planning process.[26] Planning for Computer Network Operations requires a level of expertise that is not readily available from the services. In testimony before the House Armed Services Committee, General Alexander, the commander of USCYBERCOM states, "If you were to ask me what is the biggest challenge that we currently face, it's generating the people that we need to do this mission."[27] There are a variety of reasons given for the shortage of cyber experts in the military services, but ultimately the reasons are irrelevant. It is important to understand that the shortage is not in personnel, but rather in cyber trained personnel, a distinction that seems obvious at first but one with radically different solutions. A shortage in trained personnel can be overcome in time with the appropriate training and appropriate emphasis by the services.[28] It is unreasonable to argue that a training issue that will be resolved in a few years time is the rationale for centralizing cyber expertise at USCYBERCOM. As with other shortages in specific fields, linguists for example, the services have the responsibility and capability to increase incentives for recruiting and

[26] Franklin, p 17.
[27] Alexander HASC testimony.
[28] Chilton HASC testimony.

maintaining a force. So any current shortage can be mitigated in time with the proper incentives. In the short term, existing planning staffs can be educated in cyberspace to ensure some level of experience and expertise is available to the Geographic Combatant Commander. Indeed in this case, USCYBERCOM might well benefit by pushing is most experienced personnel out to the Geographic Combatant Commands in order to alleviate the workload at both headquarters as the inclusion of a cyber expert in the J5 at the Geographic Combatant Command is likely to reduce the workload on USCYBERCOM as final products and tasks developed will be feasible.

While USCYBERCOM's mission does include a planning aspect, it also includes a requirement to support the Geographic Combatant Commander. General Alexander points out in his congressional testimony, "In general, the Commander, U.S. Cyber Command will be the supported commander for planning, leading, and conducting DOD defensive cyber and global network operations and, in general, is a supporting commander for offensive missions."[29] Support in planning for Computer Network Operations can be conducted in many ways. Planning support can certainly be presented in the form of a forward deployed planning or operations task force such at the JCOTF. The fact that USCYBERCOM has the mission of planning is actually somewhat irrelevant to the argument as the question at hand is really about how that planning is conducted. Again, this is not a discussion about command and control of planners but rather a discussion about how to best plan to ensure integration and synchronization throughout the JOPP.

Finally, the fact that USCYBERCOM has Operational Control over the forces that conduct activities in cyberspace and the reality that these limited resources can have global effects can be considered a reason for retaining planning functions at USCYBERCOM. This

[29] Alexander, Keith B., from his advance questions provided to the senate armed services committee.

will allow USCYBERCOM to prioritize its resources in support of multiple Combatant Commanders and utilize limited operational capabilities globally. Geographic Combatant Commanders should request the effects they want and allow USCYBERCOM to plan and prioritize effects to support each request.[30] However, competition between commands for high demand/low density assets is resolved by the SECDEF and not the Combatant Commanders and this approach ultimately leads to a less effective use of cyber capability on behalf of the supported Combatant Commander.

Concluding Remarks

I am just preparing my impromptu remarks – Winston Churchhill

The recognition of cyberspace as a domain will undoubtedly bring challenges for the planning staffs around the world. USCYBERCOM can bring a great deal of experience, knowledge, and thought to a planning staff at a Geographic Combatant Command. Likewise, the experience and knowledge that exists in the theater is critical to understanding the enemy and the associated time, space, and force considerations during planning. The challenge in getting the theater and cyberspace experts together in the same room to discuss their way through a planning problem can be easily overcome. This is not about command and control; it is about producing the best product for the commander. The planning team strives to integrate capabilities across all domains in order to achieve synchronization and unity of effort. A cyber planner assigned to the planning staff at the Geographic Combatant Command ultimately ensures a better product for both the local commander as well as USCYBERCOM.

[30] Franklin, p 8.

BIBLIOGRAPHY

Alexander, Keith B. "Testimony," Senate, *Advance Questions for Lieutenant General Keith Alexander, USA* http://armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf (accessed 1 October 2010).

_____. "Testimony," House, *Statement of General Keith B. Alexander, Commander United States Cyber Command Before the House Committee on Armed Services*. 23 September 2010. http://armedservices.house.gov/pdfs/FC092310/AlexanderStatement.pdf (accessed 15 October 2010).

_____. "Testimony," House, *House Armed Services Cyberspace Operations Testimony.* 23 Sept. 2010. http://www.stratcom.mil/speeches/52/House_Armed_Services_Committee_Cyberspace_Operations_Testimony (accessed 25 October 2010)

Caralli, Rich et al. *Preparing to Fight in Cyberspace* (Oakland, CA: Carnegie Mellon University, 2007)

Carey, Michael J. "Integrating and Synchronizing Non-kinetic Effects: USSTRATCOM Forward Integration Team." *High Frontier,* 6: 4, August 2010.

Chilton, Kevin P. "Testimony," House, *General Chilton's Session before the House Armed Services Committee* 17 March 2009. http://armedservices.house.gov/hearing_information.shtml (accessed 24 September 2010).

Crowell, Richard M. "Hung on the Old Bridge like Slaughtered Sheep." Newport, RI: Naval War College.

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

Gates, Robert M., Secretary of Defense, to Secretaries of the Military Departments, et al, memorandum entitled "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations" 23 June 2009.

Gray, Collin S. "Strategic Thoughts for Defence Planners." *Survival*, 52: 3, 159-178.

Mehdi Khosrow-Pour. "Advanced Topics in Information Resources Management." Idea Group Inc, 2006

Kuehl, Dan. "Information as Power." Powerpoint. National Defense University, Information Resource Management College. Washington D.C.

Markoff, John. "Before the Gunfire, Cyberattacks." *New York Times,* 12 August 2008.

Merriam-Webster. http://www.merriam-webster.com/dictionary/cyberspace (accessed 17 October 2010.

Navy Officer of Information. "U.S. Fleet Cyber Command / U. S. 10th Fleet Global Operations." http://www.navyreserve.navy.mil/Rhumb%20Lines/U%20S%20%20Fleet%20Cyber%20Command_U%20S%20%2010th%20Fleet%20Executing%20Global%20Operations%2028%20May%2010.pdf (accessed 10 October 2010)

U.S. Office of the Secretary of the Air Force. *Cyberspace Operations.* Air Force Doctrine Document (AFDD) 3-12. Maxwell AFB, AL: LeMay Center for Doctrine Development and Education. 15 July 2010.

U.S. Department of Defense "U. S. Cyber Command Fact Sheet." U.S. Department of Defense Office of Public Affairs. 25 May 2010.

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 19 August 2009.

_____. *Joint Operations*. Joint Publication (JP) 3-0. Washington DC: CJCS, 17 September 2006 Incorporating change 1, 13 February 2008.

_____, *Information Operations*. Joint Publication (JP) 3-13, Washington, DC: CJCS, 13 February 2006

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

Vego, Milan. *Joint Operational Warfare: Theory & Practice*, Newport, RI: Naval War College Press, 2007.