Strategy Research Project

A Model for Command and Control of Cyberspace

by

Colonel Jeffrey A. May
United States Army

United States Army War College
Class of 2012

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 14-02-2012	**2. REPORT TYPE** Strategy Research Project	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE
A Model for Command and Control of Cyberspace

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Jeffrey A. May

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

Mr. William O. Waddell
Center for Strategic Leadership

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution: A

13. SUPPLEMENTARY NOTES

14. ABSTRACT

A combination of the United States Transportation Command and the United States Special Operations Command model for command and control is a more appropriate model for the United States Cyber Command to direct the operation and defense of the Department of Defense networks in cyberspace. This paper will define the proposed command and control model and compare that to the current command and control model being used by United States Cyber Command. The argument will be made that cyberspace is a true joint domain and United States Cyber Command will need to control not only the networks, but also the manning, training, and the funding in order to direct the operation and defense of the United States Department of Defense networks.

15. SUBJECT TERMS
Cyber Command

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UNCLASSIFED	**b. ABSTRACT** UNCLASSIFED	**c. THIS PAGE** UNCLASSIFED	UNLIMITED	28	**19b. TELEPHONE NUMBER** *(include area code)*

USAWC STRATEGY RESEARCH PROJECT

A MODEL FOR COMMAND AND CONTROL OF CYBERSPACE

by

Colonel Jeffrey A. May
United States Army

Mr. William O. Waddell
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Jeffrey A. May

TITLE: A Model for Command and Control of Cyberspace

FORMAT: Strategy Research Project

DATE: 14 February 2012 WORD COUNT: 5,191 PAGES: 28

KEY TERMS: Cyber Command

CLASSIFICATION: Unclassified

A combination of the United States Transportation Command and the United States Special Operations Command model for command and control is a more appropriate model for the United States Cyber Command to direct the operation and defense of the Department of Defense networks in cyberspace. This paper will define the proposed command and control model and compare that to the current command and control model being used by United States Cyber Command. The argument will be made that cyberspace is a true joint domain and United States Cyber Command will need to control not only the networks, but also the manning, training, and the funding in order to direct the operation and defense of the United States Department of Defense networks.

A MODEL FOR COMMAND AND CONTROL OF CYBERSPACE

A combination of the United States Transportation Command (USTRANSCOM) and the United States Special Operations Command (USSOCOM) model for command and control is a more appropriate model for the United States Cyber Command (USCYBERCOM) to direct the operation and defense of the Department of Defense (DoD) networks in cyberspace. This paper will start by laying out the Department of Defense strategy for operating in cyberspace and then defining cyberspace as a domain. This discussion will lead to the proposed command and control model, and compare that to the current command and control model being used by United States Cyber Command. The argument will be made that cyberspace is a true joint domain, and United States Cyber Command will need to control not only the networks, but also the manning, training, and the funding in order to direct the operation and defense of the United States Department of Defense networks.

The President of the United States has stated in the 2010 National Security Strategy, “Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation”.[1] Every day international businesses, consumers, and militaries worldwide utilize cyberspace to conduct daily operations, moving assets across the globe in seconds.[2] “Domains infer that the physical dimensions of land, sea, air, and space are a battle space defined by physical properties in time and space; a place with real political, economic, and military value, where nations and actors seek to dominate their adversaries.”[3] As in the other domains, cyberspace provides a conduit for moving assets in order to affect an outcome in business as well as on the battlefield. DoD alone operates over 15,000 networks, and 7 million computing devices in dozens of countries across the globe.[4] The fact that the United States military has invested in cyberspace for command and control and weapons systems has led the former Secretary of Defense, Robert Gates, to state, “Although it is a man-made domain, cyberspace is now as relevant a domain for DOD activities as the naturally occurring domains of land, sea, air, and space.”[5] Having defined cyberspace as a domain, the Department of Defense must now devise a method to organize, train, and equip for cyberspace to support national security interest.[6]

The Untied States Department of Defense established United States Cyber Command as a Sub-Unified Command under United States Strategic Command (USSTRATCOM) in order to address cyberspace as a warfighting domain. There are five strategic initiatives in the Department of Defense Strategy for Cyberspace; the first two are relevant to the command and control of cyberspace. “Strategic Initiative 1: DoD will treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace’s potential.”[7] USCYBERCOM was given the mission of managing cyberspace risk through increased training, situational awareness, and creating secure networks as well as developing integrated capabilities with Combatant Commanders, Services (Army, Navy, Air Force, and Marines), Agencies, and the acquisition community.[8] “Strategic Initiative 2: DoD will employ new defense operating concepts to protect DoD networks and systems.”[9] This initiative directly addresses the President’s National Security Strategy statement that defending against cyber threats requires networks that are secure, trustworthy, and resilient.[10] In order to accomplish the second initiative, DoD will employ active cyber defense capabilities and develop new defense operating concepts, and computer architectures.[11] The ability of USCYBERCOM to address these two initiatives depends on the command and control structure DoD adopts for USCYBERCOM.

Having defined cyberspace as the newest warfighting domain, what does it mean to command and control cyberspace? As of the writing of this paper, Joint Pub 3-12, Cyberspace Operations, had not been approved. Therefore, according to the draft Joint Pub 3-12, cyberspace is defined as "A global domain consisting of the interdependent networks of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. "[12] Think of the cyberspace domain as roads and sea lanes connecting every city, town, and village in the world. The information that flows across the infrastructure, networks, and computer systems is like products flowing from the shipping lanes to the highways of the world. The world of Westphalian states has imposed artificial boundaries on those lines of communication that don't necessarily apply in cyberspace, however, they can apply in a state in which the government controls the internet service providers. So, as you can see, cyberspace acts like sea and land lines of communication, but the cyberspace domain knows no boundaries. This fact is one of the main concerns when discussing the command and control of cyberspace. The geographical boundaries the U.S. DoD has place on the Geographical Combatant Commanders does not apply to the cyberspace domain. What a commander does in his area of responsibility can very well affect another commander's area of responsibility half way around the world in a blink of an eye.

Cyber operations are defined as the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace.[13] There are several activities that a commander will have to execute command and control over within cyberspace operations. These activities are defensive cyber operations, offensive cyber operations, computer network exploitation, and computer network operations. Defensive cyber operations are defined as the passive and active operations to preserve the ability to utilize friendly cyberspace capabilities and protect DoD networks.[14] Offensive cyber operations are defined as activities that actively gather information, manipulate, disrupt, deny, degrade, or destroy computers, information systems, or networks through cyberspace.[15] Computer network exploitation is defined as enabling intelligence operations through the use of computer networks to gather data from an adversary's automated information systems.[16] The last definition is computer network operations which is the day-to-day operations required to run and maintain DoD networks. The issues with running and maintaining DoD networks are some of the key factors when deciding the command and control structure required for USCYBERCOM. Daily network operations and maintenance of the man-made cyberspace domain enables defensive cyber operations, offensive cyber operations, and computer network exploitation.

An agency that is essential to the operations and maintenance of the DoD networks is the Defense Information Systems Agency (DISA). DISA is a combat support agency that plans, acquires, and maintains the backbone that the DoD networks traverse.[17] DISA is a joint organization with a supporting command and control relationship to USCYBERCOM. The mission of DISA is "a Combat Support Agency; (it) engineers and provides command and control capabilities and enterprise infrastructure to continuously operate and assure a global net-centric enterprise in direct support to joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of operations."[18] DISA does the heavy lifting at the DoD level and maintains the DISA Information Systems Network (DISN) that provides the backbone for the DoD networks.

The core missions at DISA are command and control, computing/application hosting, contracting and procurement, enterprise services, information assurance, multinational information sharing, satellite communications, and spectrum operations.[19] DISA has a part to play at the national level in most everything that goes on in cyberspace. DISA's three lines of operation are enterprise infrastructure, command and control and information sharing, and operate and assure.[20] The DISA joint enablers are acquisition, contracting, engineering, information and knowledge management, people, planning, resources, spectrum, and testing.[21] It is under the line of operation of operate and assure, as well as the joint enabler of acquisition and contracting, that DISA is most important to USCYBERCOM.

"DISA's Operations Directorate coordinates and synchronizes DISA's "Operate and Assure" line of operation in support of the full spectrum of military requirements and supports USCYBERCOM in its mission to provide secure, interoperable, and reliable operation of the DoD net-centric enterprise infrastructure."[22] The Operations Directorate has a field office of subject matter experts located in all of the Combatant Commands. It also maintains the Theater Network Operations Centers (TNC), and the DISA Command Center (DCC) which all are invaluable to the daily operations of USCYBERCOM. The field offices are the link between the Combatant Commander and all the DISA capabilities. The TNC's provide regional customer service to the Theater Network Operations and Security Centers (TNOSC's). The DISA Command Center (DCC) is the command node for all the TNC's and operations taking place worldwide.

Prior to the stand up of USCYBERCOM, Joint Task Force Global Network Operations (JTF-GNO) directed the operations and defense of the DoD cyberspace domain through the Services, Combatant Commanders, and Agencies. The orders issued to the field went from the commander of JTF-GNO to the communications directorates of the Services, Combatant Commanders, and Agencies. This flow of information kept the network operators informed, but left the commanders and operations directorates out of the loop. Consequently, the commanders in the field may or may not know what was going on in the cyberspace domain. Cyberspace was not seen as commander's business. The 2008 thumb drive intrusion into DoD networks was the event that moved the business of cyberspace operations from the network operators to the commanders. USSTRATCOM called the clean-up Operation Buckshot Yankee (OBY). As Assistant Secretary of Defense William Lynn stated, "This previously classified incident was the most significant breach of U.S. military computers ever, and it served as an important wake-up call. The Pentagon's operation to counter the attack, known as Operation Buckshot Yankee, marked a turning point in U.S. cyberdefense strategy."[23] USCYBERCOM was one outcome of OBY, but another and perhaps just as important, was cyberspace becoming commander's business. Former USSTRATCOM Commander, Gen Kevin Chilton, stated that during Operation Buckshot Yankee he couldn't get answers to simple questions such as how many computers are on the DoD networks.[24] In the same 2010 speech he stated, "A year ago, cyberspace was not commander's business. Cyberspace was the sys-admin guy's business."[25]

USCYBERCOM Model

The current command and control structure for USCYBERCOM is maturing from the NetOps point of view. Currently, USCYBERCOM directs the operations of the global information grid through the Cyber Service Components. Those components are 24th Air Force, Army Cyber Command, 10th Fleet, and Marine Forces Cyber Command. GEN Alexander, USCYBERCOM Commander, has stated in his 2010 posture statement to the U.S. congress that the Service components are where the heavy lifting is done: "What we do as U.S. Cyber Command in many ways will actually get done through Army Forces Cyber Command, the Navy's Fleet Cyber Command, the 24th Air Force, and Marine Forces Cyber Command."[26] The required forces to operate the cyberspace domain are not assigned to USCYBERCOM. Those forces are in the Services, which is why USCYBERCOM directs the operations of cyberspace through the Services. In recognition of this challenge, the USCYBERCOM Commander also told the U.S. Congress that USCYBERCOM is working closely with the Joint Staff, Combatant Commands, and the Services to develop the command and control structure required over the units that belong to these Service components.[27]

USCYBERCOM has operational control over the Service components, and the Service components have operational control over the NOSC where the work of maintaining the networks is managed. Operational control is the authority over subordinate forces to organize, assign tasks, designate objectives, and provide direction necessary to accomplish the mission; it does not include direction for logistics, administration, discipline, internal organization, or unit training.[28] A good first step was to move those NOSCs under the Service components. This arrangement at least gives USCYBERCOM indirect control over the seams where the orders meet the implementers. However, the NOSCs are Service specific organizations working in a joint domain. This means that the funding is coming from the Services' Title 10, U.S. Code authority. There is the potential for Services to implement direction in a Service specific manner that does not always contribute to the ability of USCYBERCOM to defend the DoD networks. Also, other than the fact that the funding is Service specific, there is no reason to have multiple NOSCs from separate Services operating in the same area of responsibility in a joint domain. It makes more sense from a joint and fiscal point-of-view to make the NOSCs joint organizations into which units plug-in depending on the theater in which they are operating. The funding could be handled in one of two ways. First, the executive agent for that theater would provide the funding, in which case, the unit providing the service would be single Service but servicing a joint force. Second, USCYBERCOM could be given Title 10 authority to fund and man true joint NOSCs.

The relationships between DISA and the Service NOSCs would be enhanced with true joint NOSCs. The relationship between the TNC and the TNOSC should be solidified by assigning the TNC's and the DCC to USCYBERCOM. This relationship would provide USCYBERCOM with complete visibility of the DoD networks. The Geographical Combatant Commanders would obtain visibility of the networks in their area of responsibility by assigning a supporting relationship between the TNC and the theaters.

There are two other aspects to the command and control of cyberspace in addition to network operations, defensive cyber operations, and offensive cyber operations. Passive defense measures reside in the network operator (J6) area of responsibility for implementation, but active defense measures, to include response actions, as well as offensive operations are in the operations (J3) area of responsibility. The cyberspace operations that are offensive in nature follow a different chain of command from USCYBERCOM to the Combatant Commanders. USCYBERCOM has placed, or is in the process of placing, cyber support elements in the Combatant Commands in order to facilitate planning and coordination. The Combatant Commanders are also in the process of standing up joint cyber cells to work cyberspace issues. The very nature of cyberspace makes coordination and synchronization critical in order to avoid affects in another Combatant Commander's area of responsibility.

The issues with the current command and control structure for USCYBERCOM are in the control of funding, training, and execution. The Services control the funding and training of the DoD cyberspace forces. The personnel to execute operations in cyberspace also belong to the Services. USCYBERCOM provides the direction to the Services through the command and control relationship with Service components. The ability to effect operations around the world at the speed of the network requires coordination throughout DoD, as well as the interagency. The interagency consists of those elements of the U.S. government that are outside of DoD. In a man-made domain that requires constant maintenance, up-to-date security measures, highly trained operators, and coordination with the interagency, centralized control is essential in establishing an environment for success. However, centralized control is in direct opposition to how the Department of Defense fights through the Geographical Combatant Commanders.

The command and control structure, funding authority, and acquisition authority required to conduct computer network operations is crucial to successful DoD cyberspace operations. There are two models to explore when determining the best command and control structure for USCYBERCOM, U.S. Special Operations Command (USSOCOM) and U.S. Transportation Command (USTRANSCOM). Both have their advantages and disadvantages, and neither fully meets the requirements of cyberspace.

USSOCOM Model

The USSOCOM command and control model starts with Section 167, Title 10, U.S. Code, authority. This section assigns USSOCOM the same responsibilities as the Services when it comes to training and equipping the force, developing doctrine, program and budget submission, expenditure of funds, acquisition, establishing and validating requirements, and ensuring interoperability of equipment and forces.[29] In comparison, the Geographical Combatant Commanders must rely on the Services to train and equip, as well as fund, forces under their command. This Title 10 authority and resources is essential to setting the conditions for success in a man-made joint warfighting domain. Without it the DoD will continue to have service specific solutions to meet joint demands in a domain that is constantly evolving in the commercial world.

All Special Operations Forces (SOF) based in the continental United States are assigned to USSOCOM.[30] This means that USSOCOM has Combatant Command (COCOM) authority over those forces. COCOM authority provides the combatant commander the authority to perform those functions of command over assigned forces involving organizing and employing forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training and logistics.[31] In contrast, USCYBERCOM has operational control (OPCON) authority over the Service component headquarters which does not include logistics, administration, training, discipline, or organization. Essentially what this means is that those Service components OPCON to USCYBERCOM have two bosses, USCYBERCOM and the Services. This arrangement creates and environment in which Service specific solutions could continue to grow.

Within the Geographical Combatant Commander's (GCC) area of responsibility, USSOCOM has deployed a Theater Special Operations Command (TSOC). The TSOC is OPCON to the GCC and has all of the SOF in theater assigned to TSOC.[32] Applying this concept to cyberspace, the Theater Cyber Center (TCC), or as one author refers to it as the Regional Cyber Center, would play the role similar to the Theater Special Operations Command.[33] The TCC would be responsible for the operations and defense, as well as integrating cyber effects into the GCC theater plans and the interface with USCYBERCOM.[34] Currently, the GCC has several organizations to coordinate the daily operations of the network. The J6 is the primary GCC interface, and the J6 interfaces with the Theater Network Operations Control Center (TNCC), as well as the DISA TNC, and the TNOSC run by the Services.[35] The Army has a regional focus with the TNOSCs; the other Services have less of a regional approach and more of a centralized control. In the USSOCOM model, the TCC would have control over the TNCC, and the TNOSC. Furthermore, the TNOSC would be a joint organization servicing all component forces in the GCC's theater. A truly joint organization in a theater would allow the GCC to operate/organize how the command will fight on a daily basis. Currently, the GCC's have control over only their headquarters networks. The Services operate the networks for the components assigned to the GCC. USCENTCOM is the exception in the Afghanistan area of operation where they are organized the way they are fighting. All services are on the same network in Afghanistan. This makes coordination much easier within the area of operation.

The TCC would also be responsible for integrating cyberspace operations in the GCC's theater plans. The TCC would be the central point for all coordination with USCYBERCOM and the interagency for deconfliction of cyber effects.[36] The TCC would be essential for the planning process, but the very nature of cyberspace makes this arrangement problematic when it comes to execution. As has already been stated, the fact that actions in cyberspace can affect national level operations as well as other GCC operations at the speed of light, make the decentralized execution nature of the USSOCOM model less than desirable. Take for instance Operation Buckshot Yankee where an infected thumb drive was placed in a DoD computer in the CENTCOM area of responsibility, and spread to computers in other GCCs areas prior to the clean-up, which took over 14 months.[37] USTRATCOM was in charge of the clean-up, not the CENTCOM Commander. USCYBERCOM must have centralized control over the execution phase of all cyberspace operations in order to avoid adverse effects.

USTRANSCOM Model

The USTRANSCOM model for command and control would provide USCYBERCOM the required centralized control over Combatant Commander's operations that could have global unintended effects. The GCC theater command and control model for deployment and distribution falls under the GCC J4 (logistics). A Joint

Deployment and Distribution Operations Center (JDDOC) is established in order to coordinate transportation requirements within the theater and to coordinate external transportation requirements with USTRANSCOM's Deployment and Distribution Operations Center (DDOC).[38] The land and air components designate a director of mobility forces (DIRMOBFOR) to coordinate service mobility requirements with the JDDOC. The JDDOC only controls theater assets and, therefore, USTRANSCOM retains control of global assets. In applying this model to cyberspace, the JDDOC could be called a Joint Cyber Synchronization Center (JCSC) which would work directly for the GCC and coordinate with the TNOSC as well as USCYBERCOM.[39] The director of cyber forces (DIRCYBERFOR) would coordinate with the services.[40] In a C2 model where the TNOSCs were both joint and directed the service components, the DIRCYBERFOR would not be necessary. DIRCYBERFOR responsibilities would be conducted by the JCSC for both offensive and defensive operations.

The USTRANSCOM model would require some modifications in order to be useful in cyberspace but the key attribute is the centralized control of USCYBERCOM over global effects. USTRANSCOM retains OPCON of global assets and only relinquishes assets to the GCC when available and only for in theater missions. In comparison to the USSOCOM model, the GCC owns the assets in his theater. The main issues with the USTRANSCOM command and control model are with the lack of Title 10 authority. USTRANSCOM does not have the funding or training authority that USSOCOM and the Services have in order to train and equip the force. USTRANSCOM is funded through the Defense Capital Working Fund which is a fee for service arrangement with the Services. The force is also trained by the Services, and material is purchased through Service acquisition.

Proposed USCYBERCOM Model

What does right look like for the command and control of USCYBERCOM? Starting from the top, the president needs to designate USCYBERCOM as a Unified Combatant Command. USSOCOM was born out of the failure of Operation Desert Claw, the failed U.S. attempt to rescue the American hostages being held at the U.S. Embassy in Tehran, Iran.[41] From this failure, Congress tasked DoD to build the capacity to conduct special operations. The Services could not agree how to accomplish this task, and it took an amendment to the Goldwater-Nichols Act in 1987 to formally establish Special Operations Command.[42] The stakes were much higher in Desert Claw, but the same principle applies to Operation Buckshot Yankee. This cyber operation served as a wake-up call.

The Secretary of Defense has the authority to designate a sub-unified command which Secretary Gates did in 2009 establishing USCYBERCOM. USSTRATCOM has several global mission areas to include cyberspace, space, global strike, integrated missile defense, intelligence surveillance and reconnaissance, and combating weapons of mass destruction.[43] Included in the global strike mission is the nation’s nuclear deterrence mission. As a sub-unified command, USCYBERCOM must compete with the rest of the USSTRATCOM mission areas for resources. USCYBERCOM will also have to compete with the U.S. Air Force for resources since U.S. Air Force is the executive agent for USSTRATCOM, and therefore provides USSTRATCOM funding. Cyberspace is so important to the other traditional domains of land, sea, air, and space that former Secretary of Defense Gates chose to put a four star headquarters under

USSTRATCOM in order to provide cyberspace the focus required to enable the traditional domains to operate in and through cyberspace. That was a good first step, but with the current mission load of USSTRATCOM, and the importance of cyberspace to the United States, it is time to make USCYBERCOM a Unified Combatant Command.

Second, USCYBERCOM must be given Title 10 authority like the Services and USSOCOM. The first initiative in the DoD Strategy for Cyberspace is DoD will treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential.[44] Designating USCYBERCOM as a Unified Combatant Command is not enough to enable USCYBERCOM to accomplish this DoD assigned mission. By assigning USCYBERCOM Title 10, U.S. Code authority, USCYBERCOM is now responsible for the manning, training, and equipping of the DOD cyberspace forces, and will receive the funding required to execute the mission.

DoD cyberspace forces include all of the Services. The information technology that makes up cyberspace is not Service unique, and therefore inherently joint in nature.[45] The cyberspace domain is a man-made domain that is driven by the private sector in which the standards, protocols, network tools, and applications are defined. The DoD portion of the cyberspace domain was created by the Services to meet service requirements in line with chosen private sector standards. Designing to Service requirements is in direct conflict with the joint nature of cyberspace. Services funding their own acquisitions creates stove pipe solutions, and leads to non interoperability on the battlefield where the joint fight is taking place. By placing the acquisition authority for cyberspace under USCYBERCOM, the DoD is now addressing the interoperability problem from the other direction. Cyberspace systems are now developed joint, and the

Services will be required to develop their domain specific instruments of war to joint standards.

Operating and defending cyberspace is also enabled by placing the training requirement for DoD cyberspace forces under USCYBERCOM. There is absolutely no reason for Services to develop Service specific schools to train cyber warriors. In a purely joint environment driven by the private sector, DoD forces should be trained in joint schools that teach joint doctrine. Even in the traditional domains when the same piece of equipment is used by both Services there is only one school. An example was the Armor School at Fort Knox where both Army and Marine units received training for their armor units. Currently, the Services have stood up training centers to train their cyber warriors. The Air Force has established a Cyberspace Technical Center of Excellence and the Army has established their School of Information Technology. There has been some progress made in providing joint training, such as training received at the Air Force's 39th Information Operations Squadron by both Army and Coalition troops.[46]

One of the key facts that make cyberspace training inherently joint is the commercial nature of the equipment and standards. With this in mind, more emphasis must be placed on civilian certificates of training which will also help with standardizing the training the joint cyberspace warrior receives.[47]

Next, the command and control structure of USCYBERCOM should be a hybrid of USSOCOM and USTRANSCOM in order to operate and defend the joint, man-made domain called cyberspace. Already discussed was making USCYBERCOM a Unified Combatant Command and giving USCYBERCOM Title 10, U.S. Code authority for manning, training, and equipping the cyber force in line with the USSOCOM model. Now USCYBERCOM must develop the command relationships necessary to make the cyberforces truly joint. USCYBERCOM must have COCOM authority over the Theater Cyber Center mentioned earlier in this paper. The TCC would be made up of the Geographic Combatant Commander's J6 resources, as well as the TNCC assets which become assigned to USCYBERCOM and OPCON to the TCC. The TCC would be augmented with the planners, and offensive cyberspace operators required by USCYBERCOM. This arrangement will provide the TCC with the offensive cyber operations, defensive cyber operations, and network operations assets required to support the GCC through a tactical control (TACON) relationship while remaining COCOM to USCYBERCOM. TACON means the GCC has tasking authority over the TCC to accomplish missions. The TNOSC are also assigned to the TCC and provide services for all the Theater Service Component Commands. This will ensure all of the service components fall in behind one TNOSC in theater. Those service component cyber elements are assigned to the TNOSC and are TACON to the service components. The TNC previously assigned to DISA is now a USCYBERCOM asset supporting the TCC.

This command structure provides USCYBERCOM control of all cyberspace assets and ensures that the GCC is supported. This arrangement also ensures that the cyber forces do not take direction from both USCYBERCOM and their parent Service. It also addresses the issue of technical orders going to the J6 in a command, and the operational orders going to the J3 in a command. Unity of command is simplified through this construct. The collapse of all the numerous Service networks is also simplified, creating one joint network for USCYBERCOM to operate and defend. Note that USCYBERCOM's mission now goes from one of directing the operation and defense of cyberspace to one of operating and defending the DOD cyberspace.

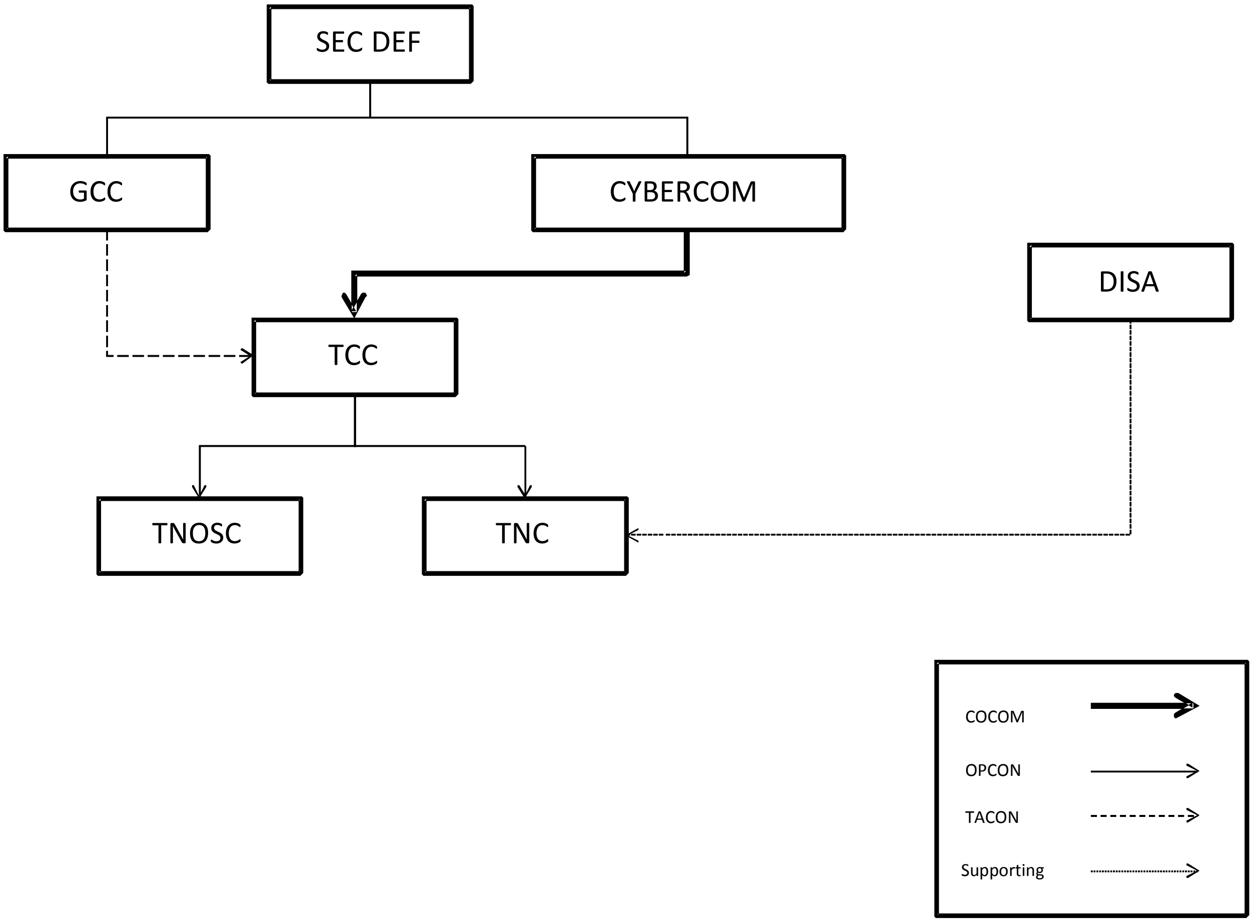

Figure 1: USCYBERCOM C2

Recommendation

In order for the U.S. DoD to effectively operate in cyberspace, there are several changes that must be made to the authority assigned to USCYBERCOM and the command and control structure that has been established for USCYBERCOM. Recommend that the President of the United States designate USCYBERCOM a Unified Command and Congress assign Title 10 authorities to man, train, and equip the joint cyber forces. Assign all Service cyber forces to USCYBERCOM. In order to provide support to the GCCs, USCYBERCOM must establish a TCC at each GCC for offensive cyber operations, defensive cyber operations, and computer network operations. USCYBERCOM maintains COCOM over the TCC while establishing a TACON relationship between the GCC and the TCC. Also, recommend collapsing the numerous Service networks into a joint network that USCYBERCOM can operate and defend. The mission of USCYBERCOM now changes from "direct" the operations and defense of DoD networks, to operate and defend the DoD network/s.

Conclusion

Cyberspace truly is a joint warfighting domain in which all of the Services depend on to fight in the land, air, sea, and space domains. The cyberspace domain was not predefined as in the case of the other domains. Cyberspace is a man made domain that continues to evolve. The defense of this domain has been made much more difficult by the way in which each Service created their portion of the domain which makes up the Department of Defense global information grid. In order for USCYBERCOM to get control of the global information grid, they must control the resources, both people and funding, required to establish and enforce the standards.

The current command and control structure for USCYBERCOM creates an environment that is joint at the headquarters level but service centric at the funding and personnel level. Funding the Services to provision their portion of the global information grid with Service specific requirements has only led to a set of non-defendable DoD networks. A vulnerability in any portion of the global information grid can lead to an adversary exploiting that vulnerability at the speed of the network, and affecting another Combatant Commander's area of responsibility on the other side of the world.

The Department of Defense must provide USCYBERCOM with the resources required to manage this man made warfighting domain. This starts with making USCYBERCOM a Unified Command with Title 10, U.S. Code authority in order to standardize this man-made domain, and to provide joint training to both the offensive and defensive operators. This model suggests a USSOCOM command and control model for USCYBERCOM from a funding and training perspective. However, USCYBERCOM must retain centralized control of a domain that has so much at stake with the other warfighting domains, and the interagency. In a domain where actions can affect so many other interests at the speed of the network, centralized control is a must. Therefore, a USSOCOM command and control model modified to retain centralized control, as afforded to USTRANSCOM, is the command and control model USCYBERCOM must have in order to operate in cyberspace. A hybrid command and control structure of Title 10 and COCOM authority, CYBERCOM planning cells and network operators in the geographic combatant commander's headquarters, and centralized control of cyberspace operations is the command and control model that USCYBERCOM must establish.

Endnotes

[1] Barack Obama, *National Security* Strategy (Washington, DC: The White House, May 2010), 27.

[2] William J. Lynn III, *Department of Defense Strategy for Operating in Cyberspace* (Washington DC: U.S. Department of Defense, July 2011), 1.

[3] Olen L. Kelley, *Cyberspace Domain: A Warfighting Substantiated operational Environment Imperative*, Strategic Research Project (Carlisle Barracks, PA: U.S. Army War College, March, 25, 2008), 19.

[4] Lynn, *DoD Strategy for Cyberspace*, 1.

[5] Robert M. Gates, *Quadrennial Defense Review* (Washington, DC: U.S. Department of Defense, February 2010), 37.

[6] Lynn, *DoD Strategy for Cyberspace*, 5.

[7] Ibid.

[8] Ibid.

[9] Ibid., 6.

[10] Obama, *National Security Strategy*, 27.

[11] Lynn, *DoD Strategy for Cyberspace*, 6.

[12] U.S Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12, First Draft (Washington DC: U.S. Joint Chiefs of Staff, December 7, 2011), GL-4.

[13] Ibid.

[14] Ibid., GL-5.

[15] Ibid.

[16] Ibid., GL-4.

[17] Alexander, *Posture Statement*, 2.

[18] *The Defense Information Systems Agency Home Page*, http://www.disa.mil/ (accessed January 14, 2012).

[19] Ibid.

[20] Ibid.

[21] Ibid.

[22] Defense Information Systems Agency, "Operations Directorate," http://www.disa.mil/About/Our-Organization-Structure/OD-HQ (accessed January 14, 2012).

[23] William J. Lynn III, "The Pentagon's New Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010), http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain (accessed December 18, 2011).

[24] Kevin P. Chilton, "2010 Cyberspace Symposium: Keynote – USSTRATCOM Perspective," May 26, 2010, http://www.stratcom.mil/speeches/2010/37/2010_Cyberspace_Symposium_Keynote_-_USSTRATCOM_Perspective/ (accessed 18 December, 2011).

[25] Ibid.

[26] Keith B. Alexander, *A Statement on the Posture of the United States Cyber Command,* Posture Statement presented to the House Armed Services Committee (Washington, DC: U.S. Cyber Command, 23 September, 2010) 2.

[27] Ibid., 2.

[28] U.S Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington DC: U.S. Joint Chiefs of Staff, November 8, 2010), 249.

[29] United States Code, Title 10, Sec 167, Subtitle A, Part 1, Chap 6, para (e)(2) and (4).

[30] U.S Joint Chiefs of Staff, *Special Operations,* Joint Publication 3-05 (Washington DC: U.S. Joint Chiefs of Staff, April 18, 2011), III-2.

[31] JP 1-02, 57.

[32] JP 3-05, III-2.

[33] David C. Hathaway, "The Digital Kasserine Pass: The Battle Over Command and Control of DoD's Cyber Forces" (Foreign Policy at Brookings: July 2011), 10.

[34] Ibid., 10.

[35] Peter J. Beim, "Network Operations: The Role of the Geographic Combatant Commands," *Information as Power: An Anthology of Selected War College Student Papers* 2, eds. Jeffrey L. Groh, David J. Smith, Cynthia E. Ayers, William O. Waddell (Carlisle Barracks, PA: U.S. Army War College, 2007), 130, http://www.csl.army.mil/usacsl/Publications/infoaspowervol2/IAP2%20-%20Section%20Two%20(Beim).pdf (accessed 14 December 2011).

[36] Hathaway, "Digital Kasserine Pass," 10.

[37] Lynn, "The Pentagon's New Cyberstrategy."

[38] U.S Joint Chiefs of Staff, *Joint Logistics,* Joint Publication 4-0 (Washington DC: U.S. Joint Chiefs of Staff, July 18, 2008), C-3.

[39] Hathaway, "Digital Kasserine Pass," 14.

[40] Ibid., 15.

[41] Bryan D. Brown, "U.S. Special Operations Command: Meeting the Challenges of the 21st Century," *Joint Forces Quarterly*, no. 40 (1st Quarter 2006): 39.

[42] Ibid.

[43] "United States strategic Command," linked from *The United States Strategic Command Home Page* at "Command Snapshot," http://www.stratcom.mil/factsheets/snapshot/ (accessed December 18, 2011).

[44] Lynn, *DoD Strategy for Cyberspace*, 1.

[45] Herbert A. Brown, “Special Operations Offers Defense Wide Lessons,” *Signal*, 60, no. 9 (May 2006): 14.

[46] Air Force News, “Cyber Training Graduates Joint Forces,” August 12, 2010. http://www.military.com/news/article/air-force-news/-cyber-training-graduates-joint-forces.html (accessed January 13, 2012).

[47] Lt. Col. David M. Hollis and Katherine Hollis, “Cyber Defense: U.S. cybersecurity must-do’s,” *Armed Forces Journal online* (February 2011), http://www.armedforcesjournal.com/ 2011/02/5432066 (accessed January 13, 2012).