Strategy Research Project

U.S. CYBER COMMAND SUPPORT TO GEOGRAPHIC COMBATANT COMMANDS

BY

COLONEL HARRY M. FRIBERG
United States Army

USAWC CLASS OF 2011

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State 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)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
02-03-2011	Strategy Research Project	

4. TITLE AND SUBTITLE

U.S. Cyber Command Support to Geographic Combatant Commands

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Colonel Harry M. Friberg

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: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Geographic Combatant Commands (GCC) do not have the structure in place to respond to Computer Network Attack (CNA) against Department of Defense (DoD) networks or to initiate Computer Network Exploitation (CNE) or CNA in response to a cyber incident in their areas of responsibility. This paper will provide the definitions required to understand the issues that confront operations in cyberspace. It will provide an overview of the legal issues, technical issues, and will provide a recommendation for the structure necessary to enable the GCCs to overcome those issues and to effectively leverage the capabilities provided by U.S. Cyber Command in support of operations within their area of responsibility. This paper recommends the creation of a Joint Cyber Functional Component Command as part of the GCC structure to integrate cyberspace operations into their contingency plans and to enable response to cyberspace incidents within their area of responsibility.

15. SUBJECT TERMS

Cyberspace, Operations, Legal, Interagency

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	26	

USAWC STRATEGY RESEARCH PROJECT

U.S. CYBER COMMAND SUPPORT TO GEOGRAPHIC COMBATANT COMMANDS

by

Colonel Harry M. Friberg
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.

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

ABSTRACT

AUTHOR: Colonel Harry M. Friberg

TITLE: U.S. Cyber Command Support to Geographic Combatant Commands

FORMAT: Strategy Research Project

DATE: 2 March 2011 WORD COUNT: 5,230 PAGES: 26

KEY TERMS: Cyberspace, Operations, Legal, Interagency

CLASSIFICATION: Unclassified

Geographic Combatant Commands (GCC) do not have the structure in place to respond to Computer Network Attack (CNA) against Department of Defense (DoD) networks or to initiate Computer Network Exploitation (CNE) or CNA in response to a cyber incident in their areas of responsibility. This paper will provide the definitions required to understand the issues that confront operations in cyberspace. It will provide an overview of the legal issues, technical issues, and will provide a recommendation for the structure necessary to enable the GCCs to overcome those issues and to effectively leverage the capabilities provided by U.S. Cyber Command in support of operations within their area of responsibility. This paper recommends the creation of a Joint Cyber Functional Component Command as part of the GCC structure to integrate cyberspace operations into their contingency plans and to enable response to cyberspace incidents within their area of responsibility.

U.S. CYBER COMMAND SUPPORT TO GEOGRAPHIC COMBATANT COMMANDS

Geographic Combatant Commands (GCC) do not have the structure in place to respond to Computer Network Attack (CNA) against Department of Defense (DoD) networks or to initiate Computer Network Exploitation (CNE) or CNA in response to a cyber incident in their areas of responsibility. This paper will address the structure required for the GCCs to leverage the capabilities provided by US Cyber Command (USCYBERCOM) in response to cyber events within their areas of responsibility.

This paper will provide the definitions required to understand the issue, will provide an overview of the legal issues confronting operations in cyberspace, and will provide a recommendation for the structure necessary to enable the GCCs to overcome those issues to effectively leverage the capabilities provided by USCYBERCOM in support of operations with their area of responsibility.

Cyberspace is defined by joint doctrine 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."[1] This definition places cyberspace within the warfighting domains of air, land, maritime, and space.[2] A definition that better supports the consideration of operations in cyberspace is provided by Joint Test Pub (JTP) 3-12 Cyberspace Operations. The JTP defines three components to cyberspace: First, the Physical Network Component that includes "all physical equipment associated with links that support the transfer of data on the network and nodes where data is created, manipulated, processed, and stored."[3] The second component is the logical network component.

> The logical elements of the network that are related to one another in a way that is abstract from the physical network components. Examples of logical network components of cyberspace are the Nonsecure Internet Protocol Router network (NIPRNET) or any website that is hosted by servers in multiple physical locations where all content can be accessed through a single Uniform Resource Locator or URL such as Defense Connect Online.[4]

The third component of cyberspace is the cyber-persona. "A cyber-persona is the next level of abstraction in cyberspace. Using the rules created in the logical network component to develop digital representations of an individual or entity in cyberspace."[5] An individual can have multiple cyber-personas, for example work and home email addresses, while an organization may only have one cyber-persona represented by its website. "This holds implications for joint forces in terms of attributing responsibility and targeting. Joint forces will require significant situational awareness, forensic, and intelligence capabilities to counter the complex threat that exists in cyberspace."[6] The three components of cyberspace, the physical network, logical network, and cyber persona provide a representation of cyberspace that allows the commander to attribute a cyber event to the geographic location where it originated, or to the individual or entity that is responsible for the event. This attribution is an essential component for successful operation in cyberspace.

DoD 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 (CNO) and activities to operate and defend the Global Information Grid."[7] CNO is subdivided into three categories, Computer Network Defense (CND), Computer Network Exploitation (CNE), and Computer Network Attack (CNA). DoD defines CND as "actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within Department of

Defense information systems and computer networks."[8] CNE is defined as "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."[9] CNA is defined as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[10] In the execution of CNO "a successful cyberattack requires a vulnerability, access to that vulnerability, and a payload to be executed. A cyberexploitation requires the same three things—and the only difference is in the payload to be executed."[11] For CNE "the delivery and execution of its payload must be accomplished quietly and undetectably—secrecy is often far less important when CNA is the mission."[12] CNE can be seen as an enabling operation prior to CNA where both operations may present legal or national defense issues.

Currently "there is no international agreement on what constitutes an act of cyber war."[13] The Law of Armed Conflict and The United Nations Charter provide the basis for consideration of the legal implications of cyber operations. The Law of Armed Conflict considers two states of being and two bodies of law. The body of law for initiation of hostilities is referred to as *jus ad bellum* (Law into War)[14] and the body of law regulating actions in war or *jus in bello* (justice in war)[15]. Prior to conflict, *jus ad bellum*, the application of the Law of War to cyber operations are dependent on the effect caused by the operation. If the effect of the cyber operation is the same as would be achieved by a kinetic attack, such as damaging power generation equipment or causing an accident that kills people, then cyber attack may be considered the same as a kinetic attack. If the attack had a lesser effect, such as making a server unavailable or

altering data, then the operation generally might not be treated as use of force. The question of evaluating a cyber attack to determine if it would constitute a use of force is the subject of "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." In the article, Michael N. Schmitt proposes six criteria for evaluating cyber attacks as armed attacks: Severity, Immediacy, Directness, Invasiveness, Measurability, and Presumptive Legitimacy. He also proposes responsibility as a seventh criterion to consider in conjunction with non-state actors. These six criteria are measured in severity across the six axis to provide a uniform framework for considering the effect of the cyber attack and whether to respond as if it were a use of force.[16] Whether the attack is considered a use of force becomes important when considering the right of self defense that is permitted without United Nations Security Council authorization. During conflict, *jus in bello*, the Law of Armed Conflict applies to cyber attack with regard to necessity, proportionality, and distinction.[17] This is further complicated in cyberspace as there is also a requirement for attribution.

> It is virtually impossible to attribute cyber attacks during the attack. Although states can trace cyber attacks back to computer servers in another state, conclusively ascertaining the identity of the attacker requires intensive and time-consuming investigation with the cooperation of the state of origin.[18]

Unfortunately the framework underpinning the Law of Armed Conflict and the United Nations Charter is for state-to-state conflict. The application is much more complicated if the attack is attributed to non-state actors. In that case the determination will have to be made whether it is a law-enforcement or national security matter.

For response to law-enforcement matters, the international community's legal regulation of cyberspace has been evolving in response to increases in cyber crime.

The Council of Europe Convention on Cybercrime came out of meetings that began in 1997 and came into force in 2004. The United States adopted the Convention on Cybercrime in 2007 and currently the other 30 nations have ratified the treaty with 17 additional nations signing the convention. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. The Convention is the first international treaty on crimes committed via the Internet and other computer networks. It deals particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.[19] The Convention was expanded in 2005 to address cyber terrorism after the events of September 11, 2001 in the United States. As part of the growing international community of interest, the United States has continued efforts to focus on cybercrime in conjunction with the United Nations which is using the Convention on cybercrime to build the framework for the International Regulation of Cyberspace.[20]

Military operations in cyberspace require understanding of the complex legal and procedural issues that have to be addressed prior to action. "US policy requires that the Armed Forces of the United States comply with the Law of Armed Conflict during all armed conflicts, however such conflicts are characterized, and during all military operations."[21] To bring the legal and procedural issues into focus at the operational level, the DoD has established Rules of Engagement (ROE) which are "directives issued by competent military authority that delineate the circumstances and limitations

under which United States forces will initiate and/or continue combat engagement with other forces encountered."[22] ROE for operations in cyberspace have to answer:

> When to execute a cyberattack—what are the circumstances under which a cyberattack might be authorized?; Scope of a cyberattack—what are the entities that may be targeted? Duration of the cyberattack—how long should a cyberattack last? Notifications—who must be informed if a cyberattack is conducted? Authority for exceptions—what level of authority is needed to grant an exception for standing ROEs?[23]

These questions form the basis for ROE in cyberspace. The current ROE is classified and addresses the authorities required to conduct operations in cyberspace at the national level. It does not address whether a cyber attack is a use of force that merits the self-defense acts that are the obligations of unit commanders as set forth in DoD doctrine which states. "Unit commanders always retain the inherent right and obligation to exercise unit self-defense in response to a hostile act or demonstrated hostile intent. Unit self-defense includes the defense of other DOD forces in the vicinity."[24] "Do non-destructive adversary probes of important military U.S. computer systems and networks (or even systems and networks associated with U.S. critical infrastructure) constitute demonstrations of hostile intent?"[25] What response is required in response to those actions? The Commander of USSTRATCOM is charged with the authority to conduct CNO in doctrine[26] and would have the obligation to respond, or to coordinate with the GCC who has the responsibility to respond to the attack in his area of responsibility. This bridge of authority for the simple act of responding in self-defense is a reflection of the complex legal and procedural issues that must be overcome for successful military operations in cyberspace. These same issues have been a source of concern for the United States government for the last two decades.

The United States Government has been focused on cyberspace since 1998 with Presidential Decision Directive - 63 (PDD-63), signed in May 1998, establishing a structure under White House leadership to coordinate the activities of designated lead departments and agencies, in partnership with their counterparts from the private sector to "eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."[27] This was updated by President Bush in 2003 with the National Strategy to Secure Cyberspace.[28] That strategy provided three strategic objectives: To prevent cyber attacks against America's critical infrastructures; to reduce national vulnerability to cyber attacks; and to minimize damage and recovery time from cyber attacks that do occur.[29] To execute this strategy, the president designated the Department of Homeland Security (DHS) as the responsible agency for cybersecurity in the United States, and charged them to lead the response to incidents within the national cyber infrastructure. Cybersecurity has continued to be one of the focus areas for President Obama. His administration used the *Securing Cyberspace for the 44th Presidency* report that was prepared prior to the inauguration to focus cybersecurity efforts. The report cited "America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration."[30] After the inauguration the administration conducted the *Cyberspace Policy Review* which was published in 2009 and includes near-term and mid-term goals to help achieve a more reliable, resilient, and trustworthy digital infrastructure for the future.[31]

The legislative branch of the United States Government has taken steps to codify these efforts into law with House of Representatives (H.R.) 4458 and Senate (S) 3480

the Protecting Cyberspace as a National Asset Act of 2010 which creates an office and director of Cyberspace Policy within the Executive Branch of government. It requires the Department of Homeland Security to establish a National Center for Cybersecurity and Communications (NCCC).

> The Director of the NCCC is charged to "work cooperatively with the private sector and lead the federal effort to secure, protect, and ensure the resiliency of the federal and national information infrastructure; and to work with the Assistant Secretary for Infrastructure Protection to coordinate the information, communications, and physical infrastructure protection responsibilities and activities of NCCC and the Office of Infrastructure Protection." [32]

These and the other provisions of the bills translate the work that has already been done by the Executive Offices of the President and the Department of Homeland Security into law.

The Department of Homeland Security, to fulfill their mission as responsible agency for cybersecurity in the United States, and to lead the response to cyber incidents within the national cyber infrastructure has established the National Cybersecurity and Communications Integration Center (NCCIC). This center is the lead for coordinating the response to cyber incidents in the U.S. and is supported by the National Security Agency and the Department of Defense as outlined in the Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity. [33] The NCCIC is augmented by the Cyber Unified Coordination Group (UCG) made up of public and private sector officials who have been pre-selected by their organizations to come together quickly to coordinate the respond to an incident. The NCCIC construct with the UCG provides the interagency and public sector representation necessary to rapidly detect, analyze, respond, and resolve cyber incidents. [34]

The coordinated interagency response to cyber incidents that is described in the National Cyber Incident Response Plan is exercised biennially and the most recent iteration, Cyber Storm III, was conducted in September 2010. Cyber Storm III brought together government agencies, 11 states, 12 international partners, and representatives from industry to exercise the National Cyber Incident Response Plan and the NCCIC. [35] The incremental successes realized in each of the Cyber Storm exercises provide valuable lessons for DoD in defining the structure to allow the Global Combatant Commands to leverage the capabilities provided by USCYBERCOM in response to cyber incidents in their respective areas of responsibility.

The Unified Command Plan (UCP) assigns areas of responsibility to GCCs who are:

> Responsible for a large geographical area requiring single responsibility for effective coordination of the operations within that area. Directives flow from the President and Secretary of Defense through the Chairman of the Joint Chiefs of Staff to the GCCs, who plan and conduct the operations that achieve national, alliance, or coalition strategic objectives.[36]

The GCCs rely on DoD networks to conduct operations in their areas of responsibility. The sum of the DoD's networks is referred to as the Global Information Grid (GIG).[37] The GIG includes the networks provided by the Defense Information Systems Agency (DISA) and the three service component networks: the Army's LandWarNet; the Air Force's C2 Constellation; and the Navy and Marine Corps' ForceNet. Each of these networks have different security and management policies that are not reconciled when the networks are brought together by DISA to support Joint Forces. Internal to the GCCs, the networks that support headquarters functions and interconnect bases are provided either by their Executive Agent service or DISA. With executive agency it would appear that within a GCC there would be only one network,

but each service has extended their service specific network into the GCC's area of responsibility to support their component forces and installations. For example, the Army is the Executive agent in US European Command[38] where it provides LandWarNet support for communications between bases and on the Army and joint bases, but on Ramstein and other Airbases C2 Constellation is provided by the U.S. Air Force, and these two service enterprise networks do not share the same security policies and are not part of the same logical network. This incongruity in policy is common within GCCs and results in difficulties in interoperability and further complicates detection and reporting of cyber incidents. This unequal application of policy within a GCC's area of responsibility and the resulting inability to conduct cyberspace operations beyond a reactive defense is a source of frustration for GCCs who see ensuring freedom of action in the cyberspace domain within their area of responsibility as their responsibility.

The response to cyber incidents within a GCC's area of responsibility follows two paths. The service Regional Network Operations and Security Center (RNOSC) reports to the supporting joint force Theater Network Operations Coordination Center (TNCC) who will inform the GCC. The RNOSC also reports the incident to the service Global Network Operations and Security Center (GNOSC) for action. The same incident is also reported by the Regional Computer Emergency Response Team (RCERT) who will also forward the report to the service Computer Emergency Response Team (CERT) in the GNOSC for evaluation.[39] The information is then passed into the intelligence domain to the National Security Agency (NSA) who has the responsibility to evaluate cyber incidents on DoD networks. The NSA will evaluate the incident and the GCC may

lose visibility of the response at that point. The NSA synchronizes their operations in the NSA / Central Security Service Threat Operations Center (NTOC).[40] The NTOC is where the GCC has to coordinate for analysis, support, and possible response to a cyber incident within their area of responsibility. The system, as it stands now, is reactive and not responsive. The result is notification that an incident occurred in the past, rather than observation of the incident in real time to enable a proactive response by the GCC. This reactive, rather than proactive, response is a source of constant frustration for the service providers and the GCCs.

The need to simplify and unify DoD's efforts in cyberspace was seen during operation Buckshot Yankee in 2008. Operation Buckshot Yankee was the response to a very serious infection of a classified network serving US Central Command that could have been dangerously exploited by an adversary if it had not been detected, analyzed, and neutralized by a combination of intelligence and military efforts. Operation Buckshot Yankee convinced leaders in the DoD of the potential for synergy that results from combining network operations with dynamic defenses and the ability to play offense in cyberspace.[41]

To unify the components of computer network operations in response to the lessons learned from Operation Buckshot Yankee and other operations, the DoD established USCYBERCOM to "link intelligence, offense, and defense under one roof."[42] USCYBERCOM is a sub-unified command under US Strategic Command with the following mission:

> USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts 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.[43]

As part of the establishment of USCYBERCOM the services are designating their service specific network providers and network defenders as service component commands subordinate to the new functional combatant command. By consolidating the network service providers and defenders under USCYBERCOM, DoD's networks will be unified to enable enterprise wide standards. At the DoD enterprise level, the creation of USCYBERCOM unifies the organizations that conducted the three components of CNO. Joint Task Force-Global Network Operations (JTF-GNO) grew out of Joint Task Force Network Defense and had responsibility for CND. The NSA-Central Security Service had responsibility for CNE as an intelligence function, and the Joint Functional Component Command for Network Warfare (JFCC-NW) which was established to conduct CNA. JTF-GNO and the JFCC-NW were deactivated and merged to form the nucleus of USCYBERCOM, which is collocated with the NSA-Central Security Service. This merger provides the cyber operations center that is bringing the components of CNO under one roof to better support national priorities and the GCCs.[44]

USCYBERCOM's Concept of Operations (CONOPS) defines three lines of operations for the command: DoD Global Information Grid (GIG) Operations (DGO); Defensive Cyber Operations (DCO); and Offensive Cyber Operations (OCO). DGO is a unified approach to architecting, building, securing, operating and maintaining the DoD networks. DCO provides unity of command and unity of effort in detecting, analyzing, countering, or mitigating threats to DoD networks. OCO is the creation of "various enabling attack effects in cyberspace, to meet or support national and Combatant

Commander's objectives and to defend DoD or other information networks."[45] These lines of operation support the unity of effort in CNO that was envisioned in the creation of USCYBERCOM.

The doctrine for how USCYBERCOM will support the GCCs is just emerging. Joint Test Publication 3-12 Cyberspace Operations is in draft and calls for coordination between the GCCs and USCYBERCOM, but is not specific or directive about the means of that coordination.[46] The USCYBERCOM CONOPS provides additional detail but is not directive in nature. It states that "USCYBERCOM will maintain continuous communications with all combatant commands to facilitate coordination, collaboration, and deconfliction of cyberspace operations as required." [47] It also states that "USCYBERCOM may forward deploy Cyber Support elements (CSEs) or Liaison Officers (LNOs) to directly support staff planning and operations as desired."[48]

> The CSEs are to "provide Combatant Command with joint operations planners and subject matter experts on cyberspace operations. The CSEs further provide interface and reach back capability to USCYBERCOM for synchronization of effects, situational awareness, and to facilitate timely threat information." [49]

The CSEs and LNOs would provide support to the GCCs, but would not represent a permanent presence in support of the command nor would they develop the situational awareness necessary to enable the GCCs to plan and conduct operations in cyberspace.

The creation of a Joint Force Cyber Functional Component Command at the GCCs is a better way to address the need to support their freedom of action in the cyber domain and would directly support USCYBERCOM's lines of operations. The precedence for the creation of a joint functional component to the GCC structure is found in the origin of the Theater Special Operations Commands (TSOCs) which were

formed to command and control Special Operations Forces (SOF) in support of the operations within the GCC's areas of responsibility. "The TSOC is the primary theater SOF organization capable of performing broad continuous missions uniquely suited to SOF capabilities. The TSOC is also the primary mechanism by which a geographic combatant commander exercises C2 over SOF."[50] The TSOC is how SOF forces are presented to the GCC and are the means to ensure that proper coordination, and support is made available to SOF forces conducting operations within the AOR. To present cyber forces to the GCC a Joint Force Cyber Functional Component Command made up of the service component cyber forces would provide a persistent USCYBERCOM presence at the GCC and would ensure unity of effort and effective command and control of cyber forces in support of DCO, DGO, and OCO. The TSOC commander has three responsibilities within the GCC. He is the Joint Force Commander, the Theater Special Operations Advisor to the Geographic Combatant Commander, and Joint Force Special Operations Component Commander.[51] The Cyber Functional Component Commander would have analogous responsibilities to the TSOC Commander: to serve as the Joint Force Commander for cyber forces in theater; to serve as the Geographic Combatant Commander's advisor on cyber operations; and to serve as the Joint Force Cyber Functional Component Command Commander for operations in the GCCs area of responsibility absent the establishment of a separate Joint Task Force.

The structure to provide for the Joint Functional Cyber Component Commands currently exists in the Army Service Component Command structure and is already part of U.S. Army Forces Cyber Command (ARFORCYBER).

> The "four Theater Signal Commands which support respectively, the U.S. Northern and Southern Commands, U.S. Pacific Command, U.S. Central Command, and the U.S. European and Africa Commands, as well as a Signal Brigade in support of U.S. Forces Korea. These forward deployed Signal Commands and the Signal Brigade are unique to the Army and give ARFORCYBER a forward network operations command and control presence in these theaters."[52]

Merging these headquarters with the Regional Computer Emergency Response Teams that are resident in support of the GCCs and U.S. Forces Korea to form the nucleus for Joint Forces Cyber Functional Component Commands is the first step in creating the new command. This initial step would be followed by assigning the other USCYBERCOM subordinate formations to ensure the successful prosecution of cyberspace operations in support of the GCCs.

The creation of Joint Force Cyber Functional Component Commands in the GCCs directly supports the lines of operations envisioned in the USCYBERCOM CONOPs. The new command provides the headquarters and authority to unify the theater's approach to architecting, building, securing, operating and maintaining the networks that support the GCC as part of a larger GIG.[53] The Cyber Functional Component Command unifies the service cyber components in the GCC to conduct DGO on a unified theater network that would operate under consistent security policies and logical boundaries allowing for the proactive network operations that the CONOPS envisions. This global unity of effort enabled by USCYBERCOM with Cyber Functional Component Commands in each GCC is required to realize the dynamic network defense operations where the command can "detect, analyze, counter, and mitigate cyber threats and vulnerabilities; to out maneuver adversaries taking or about to take offensive action."[54] This moves the theater networks from their current state where they receive notification that an attack had occurred in the past to mitigating, and responding

to attacks as they occur.[55] To play offense in cyberspace, the USCYBERCOM CONOPS envisions that the "majority of cyber operations will originate at the theater and local levels, thereby placing them under the immediate control of the GCC and its components."[56] The Cyber Functional Component Command, as part of the GCC, provides the mechanisms and reach-back into USCYBERCOM and across GCC boundaries for the horizontal and vertical coordination and the shared situational awareness that is necessary for successful offensive cyberspace operations.

Cyberspace represents one warfighting domain within the GCC's area of responsibility. To resolve the legal issues that will hinder freedom of action requires access to specialists in cyber law. The Cyber Functional Component Command would have reach back into USCYBERCOM to resolve the legal and procedural issues that operations in cyberspace pose. This reach back would enable the creation of practical Rules Of Engagement for cyberspace operations at the combatant command level that would enable freedom of action in the cyberspace domain. For issues that cross combatant command boundaries, the Cyber Functional Component Command provides a structure for coordination and escalation of legal issues for interagency coordination.

To facilitate the interagency and host-nation coordination required to conduct cyberspace operations in the GCCs areas of responsibility there will have to be a standing interagency coordination group similar to the one envisioned in the USCYBERCOM CONOPS. At the USCYBERCOM level, their CONOPS envisions the creation of a "Joint Interagency Coordination Group (JIACG) with representation from DoD, DHS, Department of Justice, Department of the Treasury, the Intelligence Community, and other agencies as applicable."[57] The roles and responsibilities of the

members of the JIACG would have to be coordinated and documented in separate interagency memorandums of agreement and support requests. This standing JIACG is required to conduct cyberspace operations, it is not an ad-hoc group that could be put together by a USCYBERCOM CSE or LNO. The CSE or LNO would not have the authority, or the regional familiarity, necessary to build the host-nation and interagency team to deconflict cyberspace operations in support of the GCC. A better model for the interagency team required to support operations in the GCCs areas of responsibility is the Unified Coordination Group that supports the National Cybersecurity and Communications Integration Center which is part of the National Cyber Incident Response Framework. A parallel group is necessary to conduct cyberspace operations outside the United States. This Theater Unified Coordination Group would be assembled by the Cyber Functional Component Command to coordinate actions in cyberspace with the host nation(s), the appropriate U.S. Embassies and our allies as an extension of the JIACG and the UCG in support of the combatant commander.

Conclusions

The structure to allow the GCCs to effectively leverage USCYBERCOM has not been defined. The current solution of providing USCYBERCOM Cyber Support Elements and liaison officer does provide adequate support for the GCCs to integrate cyberspace operations into their contingency plans, or to respond to cyberspace incidents within their area of responsibility. If the GCCs are to consider cyberspace a warfighting domain then they will need better support to overcome the legal, technical, and service parochial issues associated with conducting military operations in that domain. At the national level these issues have necessitated the creation of USCYBERCOM as a sub-unified command subordinate to USSTRATCOM to unify

operations in cyberspace. The creation of USCYBERCOM has brought together the network service providers, network defenders, the intelligence community, and military network offensive capability to unify CND, CNE, and CNA under a single headquarters. To overcome the legal and interagency coordination issues presented by conducting cyberspace operations USCYBERCOM has established a standing Joint Interagency Coordination Group to facilitate necessary coordination. This same coordination and a complementary structure will be a requirement for the GCCs to conduct cyberspace operations in their areas of responsibility. The main technical issue confronting CND in the GCCs is the disparate logical networks with multiple security architectures supporting service specific and GCC requirements within their areas of responsibility. These networks need to be unified before the GCCs and DoD will be able to move from reactive to proactive CND. For CNE and CNA the GCCs currently do not have a role short of nominating targets and waiting for feedback from USCYBERCOM or USSTRATCOM.

The creation of a Joint Cyber Functional Component Command, similar to the Theater Special Operations Command, as part of the GCC structure will provide the means to unify command and control of cyberspace operations. The Joint Cyber Functional Component Command will provide a persistent structure in the GCC to navigate the legal and technical issues that confront operations in cyberspace. The Joint Functional Component Command's reach-back into USCYBERCOM will provide the expertise necessary to advise the combatant command and to ensure that cyber operations comply with the international law.

Recommendation

To ensure the GCCs freedom of action in cyberspace and to best leverage the capability provided by USCYBERCOM I recommend the creation of a Joint Cyber Functional Component Command as part of the Geographic Combatant Command structure. This command will serve as the Joint Force Commander for cyber forces in theater; it will serve as the Geographic Combatant Commander's advisor on cyber operations; and will serve as the Joint Force Cyber Functional Component Command Commander for operations in the GCCs area of responsibility absent the establishment of a separate Joint Task Force. The Joint Functional Cyber Component Command will provide the GCC the structure necessary to leverage the capability provided by USCYBERCOM to integrate cyberspace operations in their contingency plans and to respond to cyberspace incidents within their area of responsibility.

Endnotes

[1] US Joint Chiefs of Staff, Joint Pub 1-02 Department of Defense Dictionary of Military and Associated Terms (Washington DC: US Joint Chiefs of Staff, 12 Apr 2001 as amended through 30 Sep 2010), 92, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, (accessed November 14, 2010).

[2] US Joint Chiefs of Staff, Joint Pub 1 Doctrine for the Armed Forces of the United States (Washington DC: US Joint Chiefs of Staff, 2 May 2007 with Change 1 20 March 2009), I-6, http://www.dtic.mil/doctrine/new_pubs/jp1.pdf, (accessed February 3, 2011).

[3] US Joint Chiefs of Staff, Joint Test Publication 3-12, Cyberspace Operations (Washington DC: US Joint Chiefs of Staff, 10 September 2010), I-3, http://jdies.js.smil.mil/jdeis/jel/jel/class/draft/jp3-12.pdf (accessed December 23, 2010).

[4] Ibid.

[5] Ibid.

[6] Ibid., I-3 – I-4.

[7] US Joint Chiefs of Staff, Joint Pub 1-02 Department of Defense Dictionary of Military and Associated Terms, 73.

[8] Ibid.

[9] Ibid

[10] Ibid.

[11] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, (Washington DC, National Academies Press, 2009) 81.

[12] Ibid., 81-82.

[13] Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA, O'Reilly Media, 2010), 1.

[14] Translated by http://www.latinphrasetranslation.com/translators/latin_to_english (accessed February 3, 2011).

[15] Translated by http://www.latinphrasetranslation.com/translators/latin_to_english (accessed February 3, 2011).

[16] Michael N. Schmitt, "Computer Network Attack and the use of Force in International Law: Thoughts on a Normative Framework," Columbia Journal of Transnational Law 37, No 3 (1999) 885-937.

[17] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, 33-34 and chapter 7.

[18] Carr, *Inside Cyber Warfare,* 47.

[19] Council of Europe Cybercrime Homepage, http://www.coe.int/t/dc/files/themes/ cybercrime/default_en.asp (accessed December 15, 2010).

[20] Stein Schjolberg, "A Cyberspace Treaty – A United Nations Convention or Protocol on Cybersecurity and Cybercrime" 23 March 2010, http://www.cybercrimelaw.net/documents/ UN_12th_Crime_Congress.pdf (accessed December 15, 2010).

[21] US Joint Chiefs of Staff, Joint Test Publication 3-12, Cyberspace Operations, III-13.

[22] US Joint Chiefs of Staff, Joint Pub 1-02 Department of Defense Dictionary of Military and Associated Terms, 317.

[23] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, 169.

[24] US Joint Chiefs of Staff, Joint Pub 3-33 Joint Task Force Headquarters (Washington DC: US Joint Chiefs of Staff, 16 February 2007), IV-17, http://www.dtic.mil/doctrine/ new_pubs/jp3_33.pdf , (accessed January 17, 2011).

[25] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, 169.

[26] US Joint Chiefs of Staff, Joint Pub 3-13 Information Operations (Washington DC: US Joint Chiefs of Staff, 13 February 2006), IV-1, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf , (accessed January 17, 2011).

[27] Cyberspace Policy Review, http://www.whitehouse.gov/assets/documents/Cyberspace _Policy_Review_final.pdf, 4, (accessed December 23, 2010).

[28] George W. Bush, The National Strategy to Secure Cyberspace (Washington DC: The White House, February 2003), http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf (accessed January 11, 2011).

[29] George W. Bush, The National Strategy to Secure Cyberspace, viii.

[30] Center for Strategic and international Studies, "Securing Cyberspace for the 44th Presidency," December 2008, http://csis.org/files/media/csis/pubs/081208_ securingcyberspace_44.pdf, (accessed January 29, 2011).

[31] Government Accountability Office Report GAO-10-338 Cybersecurity, published 5 March 2010, http://www.gao.gov/products/GAO-10-338 (accessed January 29, 2011).

[32] Protecting Cyberspace as a National Asset Act of 2010, S3480, 111th Cong., (June 10, 2010), Summary and status http://thomas.loc.gov/cgi-bin/bdquery/ z?d111:SN03480:@@@L&summ2=m& (accessed January 11, 2011).

[33] US Department of Homeland Security, MEMORANDUM OF AGREEMENT BETWEEN THE DEPARTMENT OF HOMELAND SECURITY AND THE DEPARTMENT OF DEFENSE REGARDING CYBERSECURITY, (Washington DC October 2010) http://www.dhs.gov/ xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf (accessed November 14, 2010).

[34] US Department of Homeland Security, *National Cyber Incident Response Plan Interim Version*, (Washington DC September 2010) 4-26

[35] "FACT SHEET: Cyber Storm III," http://www.dhs.gov/xlibrary/assets/cyber-storm-3-media-fact-sheet.pdf (accessed January 1, 2011).

[36] US Joint Chiefs of Staff, Joint Pub 1, Doctrine for the Armed Forces of the United States, I-14.

[37] US Joint Chiefs of Staff, Joint Pub 1-02 Department of Defense Dictionary of Military and Associated Terms, 154.

[38] U.S. Department of Defense Directive 5100.3, "Support of the Headquarters of Combatant and Subordinate Joint Commands" Washington, DC, 15 November 1999 Certified Current 24 March 2004. http://www.dtic.mil/whs/directives/corres/pdf/510003p.pdf (accessed January 16, 2011).

[39] Greg Rarrray, Strategice Warfare in Cyberspace, (Cambridge MA, MIT Press, 2001) 389.

[40] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, chapter 3.

[41] Keith B. Alexander, statement on *U.S. Cyber Command: Organizing for Cyberspace Operations*: Hearing before the House Armed Services Committee, 23 Sep 2010, 6.

[42] William Lynne, address on *new approaches DoD will take to defend military and civilian IT systems, delivered at the Stratcom Cyber Symposium in Omaha, Nebraska, 26 May 2010, http://www.govinfosecurity.com/articles.php?art_id=2580&opg=1* (accessed November 15, 2010).

[43] US Cyber Command Public Affairs, "US Cyber Command Fact Sheet," as of October 2010, http://www.stratcom.mil/factsheets/cc/, (accessed November 14, 2010).

[44] Keith B. Alexander, statement on *U.S. Cyber Command: Organizing for Cyberspace Operations*: Hearing before the House Armed Services Committee, 23 Sep 2010, 2.

[45] Keith B. Alexander, "USCYBERCOM CONOPS," Fort Meade MD, 21 Sep 2010, 8, https://www.cybercom.smil.mil/j5/jr%20Docs/Shared%20Documents/CONOPS/USCYBERCOM%20CONOPS%20V1_0%2021%20Sept%202010%20(Signed).pdf (accessed December 23, 2010).

[46] US Joint Chiefs of Staff, Joint Test Publication 3-12, Cyberspace Operations.

[47] Keith B. Alexander, "USCYBERCOM CONOPS," 12.

[48] Ibid.

[49] Ibid., 28.

[50] US Joint Chiefs of Staff, Joint Pub 3-05, Doctrine for Joint Special Operations (Washington DC: US Joint Chiefs of Staff, 17 December 2003), III-4, http://www.dtic.mil/doctrine/new_pubs/jp3_05.pdf (accessed January 16, 2011).

[51] Ibid.

[52] Rhett Hernandez, statement on *U.S. Army Forces Cyber Command,* Hearing before the House Armed Services Committee, 23 Sep 2010, 2.

[53] Keith B. Alexander, "USCYBERCOM CONOPS," 8.

[54] Ibid., 28.

[55] Ibid., 8.

[56] Ibid., 26.

[57] Ibid., 14-15.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu