Strategy Research Project

CYBER OPERATIONS: THE UNITED STATES ARMY'S ROLE

BY

LIEUTENANT COLONEL CHRISTOPHER L. EUBANK
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)*
16-03-2011	Strategy Research Project	

4. TITLE AND SUBTITLE
Cyber Operations: The United States Army's Role

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lieutenant Colonel Christopher L. Eubank

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

William 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

In the twenty-first century, the military added another dimension in which operations will be and should be conducted in order to deal with all the possible threats to national security. Historically, military operations were relegated to land, air, and sea, but in the last ten years, two dimensions that are more non-traditional have been added in order to be examined from a strategic, operational, and tactical perspective. First, space was added; then the cyber arena became the latest dimension opened to military operations. The role of the United States (US) Army will be one that is hard to define and execute and will be scrutinized as it grows. This paper examines the role of the US Army as this new frontier for military operations grows in importance in the future. In examining the role of the US Army, this paper will focus on the challenges of standing up Army Cyber Command through the Doctrine, Organization, Training, Material, Leader Development, Personnel, and Facilities (DOTMLPF) lens and then look at the challenge of operating in this new domain. Finally, a recommendation for ensuring that the US Army executes its mission within the cyber domain satisfactorily while facing the unknown future that includes potential personnel and budget cuts will be made.

15. SUBJECT TERMS
Cyber, Cyberwar, ARFORCYBER, ARCYBER

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

CYBER OPERATIONS: THE UNITED STATES ARMY'S ROLE

By

Lieutenant Colonel Christopher L. Eubank
United States Army

William 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: Lieutenant Colonel Christopher L. Eubank

TITLE: Cyber Operations: The United States Army's Role

FORMAT: Strategy Research Project

DATE: 16 March 2011 WORD COUNT: 5,845 PAGES: 26

KEY TERMS: Cyber, Cyberwar, ARFORCYBER, ARCYBER

CLASSIFICATION: Unclassified

In the twenty-first century, the military added another dimension in which operations will be and should be conducted in order to deal with all the possible threats to national security. Historically, military operations were relegated to land, air, and sea, but in the last ten years, two dimensions that are more non-traditional have been added in order to be examined from a strategic, operational, and tactical perspective. First, space was added; then the cyber arena became the latest dimension opened to military operations. The role of the United States (US) Army will be one that is hard to define and execute and will be scrutinized as it grows. This paper examines the role of the US Army as this new frontier for military operations grows in importance in the future. In examining the role of the US Army, this paper will focus on the challenges of standing up Army Cyber Command through the Doctrine, Organization, Training, Material, Leader Development, Personnel, and Facilities (DOTMLPF) lens and then look at the challenge of operating in this new domain. Finally, a recommendation for ensuring that the US Army executes its mission within the cyber domain satisfactorily while facing the unknown future that includes potential personnel and budget cuts will be made.

CYBER OPERATIONS: THE UNITED STATES ARMY'S ROLE

> Why is this important to the Army? ARFORCYBER provides the Army an organization capable of cyberspace operations to support our nation and warfighters in the 21st century. The new command capitalizes on existing Army cyber resources, but provides unity of effort and command by realigning current Army cyber resources under a single command. This ensures policy, force structure, capabilities development, resources and personnel within the Army will be able to operate safely, securely and effectively in cyberspace at the tactical, strategic and national levels.
>
> STAND-TO! Edition: Friday, July 2, 2010

The formation of US Cyber Command (USCYBERCOM) and the different services cyber organizations is in reaction to the cyber world becoming a more important environment within the 21st-century. The addition of the cyber domain or commons to the traditional domains of air, sea, land and space is in response to the emerging threats within the world today. To amplify the importance of this domain the President of the United States' declaration that it is an extremely important area for the future security of the United States allowed these organizations to stand up with little pressure from bureaucracy of politics. "Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation….Our digital infrastructure, therefore, is a strategic national asset, and protecting it-while safeguarding privacy and civil liberties-is a national security priority."[1] Historically, military operations were relegated to land, air, and sea; but in the last ten years, two dimensions that are more non-traditional have been added for operations. As stated in the abstract, space was added and then cyber became the last dimension added to military operations. Each of the services are still struggling to grasp what this new dimension will mean in the future of operations. The role of the Army will be one

that is hard to define and execute, but one of great importance. This paper examines this role of the Army as this new frontier for military operations grows in importance in the coming years. In examining this role, the paper will focus on the challenges of standing up the Army Cyber Command using the DOTMLPF lens as well as examining the challenges operating in this new domain. Finally, the paper will recommend a way ahead for ensuring that the US Army executes its mission within the cyber domain, satisfactorily all while facing the unknown future that includes potential personnel and budget cuts.

Background

Why a USCYBERCOM, and further yet, why a United States Army Cyber Command (ARCYBER)? As we look back through history, we will uncover why this command is necessary. Is the cyber or virtual world worthy of a separate organization within the Department of Defense (DoD) and the US Army, or is this a case of being paranoid about something that we do not really understand? Let us examine how the cyber environment has changed and grown over the last fifteen years and where we are headed in the next five years and we will then understand why these organizations are so important to the national interests of the United States.

First, let us define cyber from a couple of different viewpoints, the traditional definition and the DoD definition. Webster's Dictionary defines cyber as "of, relating to, or involving computers or computer networks (as the Internet)."[2] Before we look at how this domain came to being let us look at the DoD definition. The DoD definition is, "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."[3] As you can see both definitions are very similar, to the point that the DoD has taken the Webster's definition and just expanded it so that it is more inclusive of all things cyber. Let us further define cyber to include how the DoD defines cyber operations: "The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid (GIG)."[4] The first known use of this word was in 1991, which is very interesting since the design of the internet was completed in 1973, but it was not until 1983 that an actual network was established worldwide. Therefore, the concern over the cyber domain might be warranted since it has grown exponentially every year since its inception back in 1983. In 1995, there were approximately 16 million internet users and this grew to 458 million users in 2001. In 2009, there were 1.7 billion users. What is even more amazing is that by 2015, the number of internet hosts is expected to exceed the number of humans on the earth. The thing to remember is that not all these users are good people utilizing the cyber world for information gathering and sharing, shopping, and social networking; there are some entities in the world that will use this environment to do harm to the world and more importantly the United States. Even more important is that the organizations responsible for the security of the United States of America, the Department of Homeland Security (DHS), DoD and more specifically the US Army rely heavily on this environment to conduct their missions. Without this environment, these organizations could not effectively provide for the security of the nation. The DoD very heavily invested in the internet and the cyber world in order to conduct its mission

worldwide. As we will examine later on there are some challenges to how we operate in this environment, which make it a very complex area to conduct operations both offensive and defensive.

Now that we have defined cyber as best as we can, we will now examine the history of the both USCYBERCOM and more specifically ARCYBER and how the organizations that are tasked with securing this very uncertain and complex environment were created. So why was all this created? Secretary Robert M. Gates, the Secretary of Defense, distributed a memorandum in June of 2009 that stated this command would become operational in order to secure what was believed to be a very important and vulnerable domain.

> Yet our increasing dependency on cyberspace, alongside a growing array of cyber threats and vulnerabilities, adds a new element of risk to our national security. To address this risk effectively and to secure freedom of action in cyberspace, the Department of defense requires a command that possesses the required technical capability and remains focuses on the integration of cyberspace operations. Further, this command must be capable of synchronizing warfighting effects across the global security environment as well as providing support to civil authorities and international partners.[5]

The memorandum goes on to direct the Commander of United States Strategic Command to stand up USCYBERCOM in order to accomplish everything that he put forth in the beginning of the memorandum. What is even more significant is that Secretary Gates goes on to establish initial operating and full operating capability dates and also directs the disestablishment of the Joint Task Force-Global Network Operations (JTF-GNO) and the Joint Functional Component Command-Network Warfare (JFCC-NW) in order to create the backbone of USCYBERCOM. Why is this significant? Well essentially all network operations that the Commander, Defense Information Systems Agency (DISA) was responsible for now belong to the

Commander, USCYBERCOM. This is a monumental shift in how operations were being conducted and now the DISA is solely responsible for network and information assurance technical assistance. The JTF-GNO stood up in 2004 with its history rooted in computer network defense and operations dating all the way back to 1998. The JFCC-NW activated in 2005 with its history in computer network attack. All of these organizations were deactivated, as they became the nucleus of USCYBERCOM. Therefore, as you can see there were many significant movements in order to stand up USCYBERCOM and it was even more challenging as each of the services stood up their organizations.

ARCYBER was formed from several different organizations that already existed and had a role in the cyber domain. The three Army organizations that have a stake in the cyber domain are Space and Missile Defense Command (SMDC), Intelligence Support Command (INSCOM), and the Network Enterprise Technology Command (NETCOM). Each of these can claim that they own cyber from an Army perspective, but truth in lending is that none of them owns the domain, but each of them has part of the domain. SMDC is the proponent for the Army's space programs and utilization, which is the primary transport mechanism for all of the data traffic for the military. INSCOM is the proponent for intelligence and information operations within the Army and, therefore, much of what they do is conducted within the cyber domain, making them heavily invested in this domain. Lastly, NETCOM is responsible for the maintenance and operation of the Global Information Grid where all of this information and network traffic flows. As you can see each of these organizations can claim to be the one organization that should be responsible for cyber from the Army's perspective,

but it is really all three. They all are part of the creation of ARCYBER. Now that we examined the history of USCYBERCOM and ARCYBER let us look at the current situation within these organizations focusing on ARCYBER and the roles it plays in this new operating environment.

Current Situation across the Services

USCYBERCOM became fully operational in its new headquarters at Fort Meade, Maryland in October of 2010. In its stand up, it subsumed the Joint Task Force-Global Network Operations as the nucleus of its operations center allowing for a seamless transition of operations from DISA to the new organization. Therefore, in little over a year from Secretary Gates' directive, USCYBERCOM is conducting its mission of providing cyber security. This did not come without any challenges, some of which are still being addressed. They are similar to the challenges that ARCYBER is facing today. These challenges really lie in ownership of mission, establishment of forces and standing rules of engagement (SROE). All of these challenges are extremely difficult and providing solutions is proving to be very difficult as well. The key to conquering these challenges is creating organizations with clear mission statements and priorities in the defense of the nation through the cyber domain.

As USCYBERCOM struggles, it makes sense that its service components might struggle as well. This next section will give an overview of each of the services construct and roles and then go more in depth into ARCYBER, its organization and its mission. The first aspect to remember is that each of the services was directed to stand up a cyber component command that is subordinate to USCYBERCOM. Therefore, each organization has a dual role with responsibility to their respective service as well

as USCYBERCOM. They each stood up their organizations without an increase in service size drawing on existing personnel and units to create these organizations and accomplish the mission. Let us begin with the Air Force mainly because they were first to formally stand up this capability, and led the way in establishing their organization in support of the cyber operations effort. The Air Force Cyber Command Provisional (AFCYBER(P)) stood up in October 2008, designated the 24th Air Force at Lackland Air Force Base in San Antonio, Texas. The Air Force created this organization from units that already existed causing some consternation among units losing forces, but allowing for a more rapid establishment of capability.

The Navy also created their cyber command from existing organizations, and they leveraged both the intelligence and communications communities by merging them into an Information Dominance Organization designated 10th Fleet. The Navy decided to locate this organization at Fort Meade, Maryland to be close to USCYBERCOM. The most interesting aspect of 10th Fleet is that it operationally controls all pieces of the Navy's piece of the cyber domain. "Tenth Fleet has operational control over Navy information, computer, cryptologic, and space forces."[6] This approach has limited the internal organizational strife within the Navy although it is not perfect.

Next is the Marine Corps, which stood up the Marine Corps Forces Cyber Command at Fort Meade, Maryland in January 2010. The Marines also utilized existing units to make up the core of this new command but it is strictly dedicated to the cyber mission as stated by Lieutenant General George J. Flynn, its commander. "Pure cyber resources are comprised of an operational headquarters activity, the MARFORCYBER

Command Element; the Marine Corps Network Operations Security Center (MCNOSC); and finally, the Marine Corps Cryptologic Support Battalion's (MCSB) Company L."[7]

The Army's Role

Last but definitely not least is the ARCYBER organization and its role in the cyber domain. In this section, the focus will be on the challenges that ARCYBER is facing in standing up the unit to accomplish the mission through the lens of DOTMLPF as well as operationalizing this new domain across the Army. This section of the paper will define ARCYBER's mission and then examine how it intends to tackle the DOTMLPF challenges and its operational challenges. The first of these topics discussed is defining the mission of ARCYBER since it is straightforward, although, not easily accomplished. According to the United States Army Campaign Plan DP 141 the mission of ARCYBER is: "…plans, coordinates, integrates, synchronizes, directs, and conducts network operations and defense of all Army networks; when directed, conducts cyberspace operations in support of full spectrum operations to ensure US/Allied freedom of action in cyberspace, and to deny the same to our adversaries."[8] The Chief of Staff of the United States Army, General George Casey, has approved this mission statement. Within this mission statement, there are four components to ARCYBER operations: cyber situational awareness, cyber network operations, cyber warfare, and cyber support as seen in the figure below pulled from TRADOC Pamphlet 525-7-8, The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028, dated 22 February 2010.

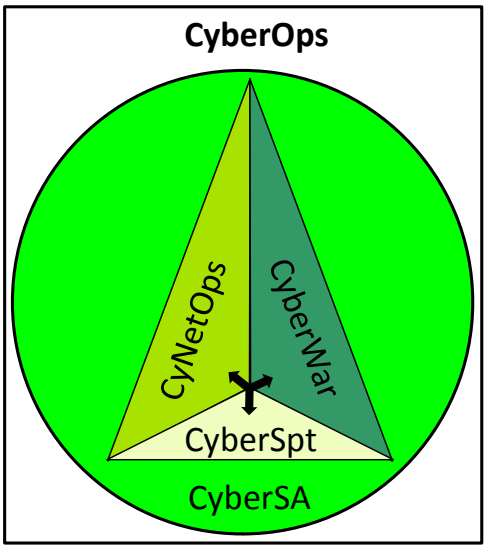

Figure 4-1. The four components of CyberOps

This concept is simple enough, but is not complete and has been further refined. According to ARCYBER, the components of cyber operations should build, operate, defend, exploit, and attack[9], with exploit and attack being the offensive elements. Each of these components is the responsibility of ARCYBER, which has recently established its own proponency directorate allowing for a seamless execution of operations within the cyber domain. The current ARCYBER commander sees challenges, but nothing that cannot be overcome with synchronized efforts across ARCYBER and USCYBERCOM.

As you can see, the mission statement and its four components include all facets of cyber operations; therefore, it affects how the organization was constructed. The Department of the Army Staff developed four courses of action for the stand up of ARCYBER, which led to the current organizational structure. The four courses of action were 1) the space community through SMDC become ARCYBER, 2) the intelligence and information operations community through United States Intelligence Support

Command (INSCOM) be the nucleus for ARCYBER, 3) the Signal Corps through United States Army Network Enterprise Technology Command be the organization that becomes responsible for cyber, and 4) a hybrid organization formed out of all three of the previously mentioned organizations. The Chief of Staff of the Army approved a hybrid organization, which was created out of the existing organizations that all have a stake in the cyber domain. This is exactly what each of the other services did to stand up their respective cyber command.

Concerning doctrinal development, there was no existing Army cyber doctrine, requiring it to be created by examining the existing doctrine for computer network defense and attack, and evolving it to encompass all the facets of the cyber mission. The bigger challenge was integrating this into existing doctrine for full spectrum operations, according to MG Hernandez, the ARCYBER Commander. "As the Army integrates cyberspace into current and future force structure and operational concepts, we must meet the challenge of how to integrate our efforts into full spectrum operations and address both the generating force and the operating force."[10] Once the doctrine is integrated into full spectrum operations, it is imperative that it continues to develop through lessons learned so that we stay ahead of the ever evolving and intelligent adversary both physically and mentally.

> Our Nation, the DoD, and the Joint Warfighters will require new and updated policy, concepts, and doctrine to effectively combat intelligent, evolving adversaries who are leveraging cyberspace to enhance their capabilities. To fight and win future battles, we must not only out-maneuver our potential adversaries, we must out-think them strategically, operationally, and tactically.[11]

Following the DOTMLPF construct, organization and its affect on ARCYBER's structure and mission is the next part to examine. First, the organizations that make up

ARCYBER already exist, but are in need of restructuring from a personnel, training, and material perspective, which will be discussed later. The second issue is the organization of the ARCYBER headquarters and how it will command, control, and work to synchronize all Army cyber operations. Referencing the courses of action for the stand up of ARCYBER mentioned earlier in this paper, the units that were brought together to form ARCYBER are key to how the headquarters is constructed and functioning. The commanding general for NETCOM is the deputy-commanding general for network operations and defense and the commanding general for INSCOM will serve as the deputy-commanding general for network warfare. All of these entities are synchronized through the Army Cyber Operations and Integration Center (ACOIC). This center is the key to operationalizing cyber operations across the force. Last is the piece of organization that is tied to every unit in the US Army. As a part of organizational structure, cyber operations must be integrated into everyday operations across every type of unit in the Army so it can help combat threats to the cyber domain as they arise.

The next function to examine is training, which includes the education of the force. The reason we need to invest in this training is our dependency on the cyber domain to conduct our day-to-day operations within the Army. "Our national and military dependence on the cyber domain and information technology demands that we invest in cyber capabilities to grow the skills necessary to maintain our ability to operate freely in cyberspace."[12] As the cyber domain grows more important as a global commons and the DoD relies on it more heavily, it is imperative that the ARCYBER invest in educating the personnel that will be working to protect and defend this borderless domain. "We

must therefore make significant investments in education, training, and experience to understand emerging trends, develop and deploy new capabilities, and effectively defend against new cyberspace threats."[13]

Next in the DOTMLPF construct is material. The material that ARCYBER utilizes already exists; the biggest challenge is keeping up with change. "To fully leverage cyberspace as a domain, we must constantly strive to harness new technologies. To do this, ARFORCYBER will pursue innovative Army acquisition processes that allow us to keep pace with rapidly changing technologies without risking the fiscal integrity of the acquisition system."[14] This does not sound hard, but in the cyber domain, material and equipment are changing every twenty-four months, which is more realistically like every twelve months. This exponential growth makes it difficult to keep the material relevant to the changing environment.

Following material is leader development, which is inherently tied to training. However, the more important aspect is helping leaders across all Army formations understand cyber, how it affects all of their operations, and how it can be a force multiplier in their battle space. Commanders at all levels must understand that cyber is a domain and therefore must be thought about during the planning phase all the way through the execution phase. These combatant and operational commanders must see the cyber domain and its forces as not only a service provider, but also a force multiplier in all operations. This requires a paradigm shift in thinking across the force; the signal and military intelligence communities' leadership must understand their changing role in order to reinforce the new mission set for these cyber forces.

The next facet of DOTMLPF is one of the most important ones in regards to getting ARCYBER at full operating capability. The personnel aspect of standing up a cyber organization is one of the hardest and most time-consuming pieces to accomplish. “This is going to take time for us to generate the force. 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.”[15] In ARCYBER, the personnel are essential to making sure that this new domain is managed properly allowing full spectrum operations to take place. These personnel do not just include the cyber personnel, but the users of the cyber domain as well. “People, however, are the centerpiece for all efforts to improve our ability to operate effectively in cyberspace. The first line of defense in cyberspace is the user. To operate effectively, we must change our culture. Every individual must understand cyberspace is a contested environment that must be protected.”[16] To augment the user, the professional cyber force must be created and trained, and once trained Army leadership must determine how we are going to retain them in the Army. “The second line of defense is our corps of cyber professionals who defend our networks and ensure operations. We will win the contest in cyberspace as we win on traditional kinetic battlefields, with the best-trained and most professional personnel. To that end, we must increase our capacity to grow cyber professionals and to retain them.”[17] This professional cyber force exists in small numbers now in the existing signal and military intelligence branches within the Army, but it needs to grow both in numbers and in expertise in order to keep up with the threats to this new domain.

The last facet is facilities. Facilities are not as difficult as some of the other facets, but are very important. The key is to ensure that all facilities are ready to

support cyber operations. The most important of these facilities are the regional and geographic operations centers. These facilities include places like Theater Network Operations and Security Centers (TNOSCs), Regional Computer Emergency Response Teams (RCERTs), and Network Enterprise Centers (NECs). Each of these facilities is in operation today, but would need to be upgraded on the technology side as well as be integrated into full spectrum operations so that commanders can leverage them through their cyber forces at all levels. Once they are upgraded and integrated into the operations, they must be placed into the appropriate command structure in order to best facilitate accomplishing the cyber mission.

As illustrated there are some significant challenges to standing up an organization using the DOTMLPF construct, but it can be done and is done all the time. As the ARCYBER Command stands up and gains full operating capability, it must utilize a lot of existing structure, personnel and doctrine while simultaneously adding to each of these facets so that it can meet its mission requirements as well as supporting commanders at all levels with the best available assets. The bigger challenge will be retaining the cyber professionals that are developed and keeping up with the technology that the adversary might use to pose a threat.

Although the DOTMLPF construct is challenging, it is only one piece of ARCYBER's problem in conducting cyber operations. The bigger challenge is operationalizing this force once it is manned, equipped, and trained for their mission. There are several challenges that must be met in order to achieve an operational force that is ready to deal with the threats within the cyber domain. These challenges start with understanding the environment, to include seeing the enemy, the terrain and

ourselves. This will entail establishing a cyber common operational picture (CCOP). In establishing this CCOP, it must be integrated into the overall common operational picture (COP) so that the commanders understand what effect; both good and bad, cyber is having on operations. To do this, the Army must first be able to "see" its networks so that those networks can be more easily defended.

> Fundamental first steps in achieving these goals include improving our ability to see and understand our networks better. We will do this by collapsing our networks from a disparate, loose federation into one Army enterprise network. This will enable us to establish centralized control of our networks and give us more complete, integrated visibility into them. Having accomplished this, we can then establish an active defense in depth across the network.[18]

Once ARCYBER can see its networks better and better defend them, they will be able to learn the enemy and terrain better. The key to this is understanding that the terrain is unrestrained and crosses multiple boundaries. This makes the cyber domain a very complex and uncertain environment, making operations even more challenging than in the traditional domains. Because of the nature of cyber threats, adversaries are harder to track and the scope of consequences from cyber activity are hard to predict.

> Future challenges will include the speed and consequential global impact of events in cyberspace. The boundaries of cyberspace are, of course, often unclear. Several factors (e.g. ownership of equipment, users of equipment, and location of equipment) influence the interpretation of where cyberspace boundaries lie. To further complicate such determinations, a cyberspace event may simultaneously occur in multiple geographic locations.[19]

The key to seeing the enemy, the terrain, and ourselves is being able to manage all of that information in one location and then pass that information to all units that need it across the battle space. In order to use the CCOP to its fullest potential, you must have a command and control structure that manages the CCOP and ensures that the information is analyzed, synthesized, and distributed to all organizations at the speed of

the network. The organization that will lead this effort is the ACOIC; the command and control center for ARCYBER responsible for ensuring all US Army units and personnel receive the information necessary to conduct full spectrum operations in cyberspace. "The ACOIC is the command and control center for all Army service-related cyberspace activities. Using current and evolving doctrine and lessons learned from enduring and future operations, the ACOIC will ensure Army personnel at all levels receive clear, concise, and timely direction to execute full spectrum operations in cyberspace."[20] Although the ACOIC will command and control all things cyber for the Army and will play a vital role in ensuring USCYBERCOM is up to date on everything going on in the cyber domain. The bridge between the Army and the joint world is a concept worth noting known as the Joint Cyber Component Command (JFC3). (This has also been discussed in other DoD circles as the JFCyCC.)[21] The concept is that as Joint Task Forces stand up and each of the component commands is created, a JFC3 or JFCyCC would be organized to manage the cyber domain and all of the forces within the domain. This would ensure that both offensive and defensive actions were being taken to ensure freedom of maneuver within this piece of battle space. The use of a JFC3 and how it executes operations is extremely important as the cyber domain becomes more important to the operations of the United States, its allies, and its adversaries especially since the DoD is a huge user of the cyber domain. The JFC3 would provide the JTF Commander with a CCOP allowing him to understand what was happening in cyberspace. Having this situational awareness allows the JTF to use offensive cyber operations to engage the enemy without putting any personnel in harm's way, as well as limiting civilian casualties and collateral damage. When you look at the conflicts of

today this is a huge leap forward in the way that engagements are fought, and would allow for different options against the adversary. It must be remembered that the enemy also has this domain at their disposal as well, and that is why we must move forward in gaining superiority in the cyber domain. This JFC3 would connect the JTF Commander to the Geographic Combatant Commander and to USCYBERCOM allowing for better situational awareness across the cyber domain.

There is still one last challenge in operationalizing the cyber domain, and that is the aspect of authorities. The definition of authorities in regards to the cyber domain is whether the DoD has permission to conduct operations outside of their own networks. This includes both computer network attack and defense, but really is concerned with the attack portion of operations. The DoD must clearly understand the United States laws and must be given permission to conduct offensive operations within the commercial and private sector when a threat is detected. These authorities must be clear so all entities involved understand what they are allowed and not allowed to do during a cyber operation. This is extremely important since cyber is a domain that has no boundaries and operates at the speed of electrons.

> Future challenges will include the speed and consequential global impact of events in cyberspace. The boundaries of cyberspace are, of course, often unclear. Several factors (e.g. ownership of equipment, users of equipment, and location of equipment) influence the interpretation of where cyberspace boundaries lie. To further complicate such determinations, a cyberspace event may simultaneously occur in multiple geographic locations. The ACOIC will assist the USCYBERCOM Joint Operations Center to maximize global availability of cyberspace for the DoD and its coalition partners and allies.[22]

All of these challenges must be faced and answered so that the cyber domain does not become a domain where there are no guidelines and therefore there is no action. The DHS and DoD, along with Department of Justice (DoJ) and the lawmakers must identify

authorities and boundaries so that the seams of the cyber domain do not go unprotected because that would be catastrophic for the United States and the rest of the world.

Conclusion

The environment in which the DoD and the Army is operating in today is very diverse and rapidly changing. One of the biggest changes in the operational environment and potentially one of the biggest challenges is the cyber domain. Currently we are beginning to set the conditions for how the DoD and the Army are going to operate within this new and unique domain. The Army's stand up of ARCYBER has laid the groundwork for the development of an organization that will conduct both offensive and defensive operations across the cyber domain in support of the DoD. This is a good beginning but it is only scratching the surface of what needs to be done to ensure that everything within the cyber domain remains protected. The United States must remain operational across the cyber domain allowing for what is considered normal day-to-day life to carry on uninterrupted. The Army is gathering all of the right personnel and expertise to fight and win within this domain, but there is still work that needs to be done.

The key to the effectiveness of ARCYBER is to ensure that Army doctrine reflects how cyber effects all operations and is part of full spectrum operations. Once all commanders understand that the cyber domain is not just a defensive one, but is offensive and can and will be a force multiplier, then the domain will have relevance. The big component to make all of this succeed is the ACOIC and its ability to provide a CCOP to all the forces within the US Army and DoD. One concept that allows this

situational awareness to be shared seamlessly throughout the force is the use of the JFC3 under all JTFs around the globe. The use of JFC3s allows for seamless, uninterrupted information within the military's portion of the cyber domain allowing all forces to use the domain to its advantage both offensively and defensively. The JFC3 will provide this situational awareness to the JTFs by using the its cyber tools developed through DOTMLPF and industry, to create the CCOP. The JFC3 can then use the network to keep the CCOP updated near real time allowing the JTF Commander to make decision and execute operations based on the status of the cyber domain. As we move into the future, we must protect our piece of the cyber commons and all of its components as well as its users, or the results could be catastrophic. It is incumbent on ARCYBER, USCYBERCOM, and the DoD to provide the security necessary for the cyber domain. It is also incumbent for Congress and the administration to support these cyber organizations as they move forward securing the cyber domain. The world is only becoming more reliant on the cyber domain and information technology; if we cannot provide the American people the security of this domain and the protection that they deserve they will quickly lose their confidence in the greater national defense system. The American people deserve the best security and protection, which includes cyberspace, and the organization that is going to deliver that security, is ARCYBER as long as they are enable to conduct their mission.

Endnotes

[1]Barack H. Obama, Jr., National Security Strategy Washington, DC: The White House, May 2010, 27.

[2] Webster's Dictionary, http://www.merriam-webster.com/dictionary/cyber.

[3] Christopher J. Castelli, Inside the Air Force, http://integrator.hanscom.af.mil/2008/May/05292008/05292008-24.htm.

[4] Deputy Secretary of Defense Memorandum, Washington DC: Office of the Secretary of Defense, October 2008.

[5] Robert M. Gates, Memorandum for Secretaries of Military Departments, Washington, DC: Office of the Secretary of Defense, June 2009, 1.

[6] Wikipedia, http://en.wikipedia.org/wiki/United_States_Tenth_Fleet, 27 December 2010.

[7] Flynn, George J."Statement of LtGen George J. Flynn, Deputy Commandant for Combat Development and Integration, Before the Subcommittee on Terrorism, Unconventional Threats, and Capabilities of the House Armed Services Committee Concerning Operating In the Digital Domain: Organizing the Military Departments For Cyber Operations". House Armed Services Committee. http://cryptome.org/dodi/marines-cyber.pdf. (23 September 2010).

[8] US Army Chief of Operations (G3/5/7), United States Army Campaign Plan DP 141, Version 29 DL, 1 February 2010, 3.

[9] Army Cyber Command/2nd Army AFCEA NOVA IT Day Presentation, “Transforming the Army Enterprise to Support the Warfighter, Tysons Corner, VA, 9 December 2010, 4.

[10] MG Rhett Hernandez, “Statement of Major General Rhett Hernandez, USA, Incoming Commanding General, U.S. Army Forces Cyber Command Before the House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities, 2nd Session, 111th Congress,” (Washington DC: 23 September 2010), 11.

[11] Ibid, 11.

[12] Ibid, 8.

[13] Ibid, 8.

[14] Ibid, 10.

[15] General Keith Alexander, “House Armed Services Committee, Cyberspace Operations Testimony”, http://www.stratcom.mil/speeches/2010/52/House_Armed_Services_Committee_Cyberspace_Operations_Testimony/, 23 September 2010.

[16] MG Rhett Hernandez, “Statement of Major General Rhett Hernandez, USA, Incoming Commanding General, U.S. Army Forces Cyber Command Before the House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities, 2nd Session, 111th Congress,” (Washington DC: 23 September 2010), 6.

[17] Ibid, 6.

[18] Ibid, 5-6.

[19] Ibid, 7-8.

[20] Ibid, 7.

[21] Major Martin Stallone, “Don’t Forget The Cyber! Why the Joint Force Commander must integrate cyber operations across other war fighting domains, and how a Joint Forces Cyberspace Component Commander will help,” (Newport, R.I.: 4 May 2009), iv.

[22] Ibid, 8-9.