Strategy Research Project

Operationalizing Army Cyber

by

Lieutenant Colonel Brian J. Lieb
United States Army

United States Army War College
Class of 2013

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
xx-03-2013	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Operationalizing Army Cyber

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Brian J. Lieb
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Dr. Andrew Hill
Department of Command, Leadership, and Management

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: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5,933

14. ABSTRACT

The United States Army must conduct further organization design in order to operationalize ARCYBER. The current organization, manning, and operating construct are not aligned to optimize the performance of the organization. The Army has current models and approaches in other existing organizations that can be used to further enhance the ARCYBER headquarters and operating forces.

15. SUBJECT TERMS
Cyberspace, Cyber Operations, Cyber Manning

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)*
UU	UU	UU	UU	32	

USAWC STRATEGY RESEARCH PROJECT

Operationalizing Army Cyber

by

Lieutenant Colonel Brian J. Lieb
United States Army

Dr. Andrew Hill
Department of Command, Leadership, and Management
Project Adviser

This manuscript 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

Title:	Operationalizing Army Cyber
Report Date:	March 2013
Page Count:	32
Word Count:	5,933
Key Terms:	Cyberspace, Cyber Operations, Cyber Manning
Classification:	Unclassified

The United States Army must conduct further organization design in order to operationalize ARCYBER. The current organization, manning, and operating construct are not aligned to optimize the performance of the organization. The Army has current models and approaches in other existing organizations that can be used to further enhance the ARCYBER headquarters and operating forces.

Operationalizing Army Cyber

The attack on Pearl Harbor on December 7, 1941 by the Japanese Imperial Navy cost more than 2400 U.S. lives and severely damaged the U.S. Pacific Fleet. The terrorist attack on September 11th, 2001 killed just under 3,000 people and cost the U.S. economy somewhere between three and five trillion dollars. The Japanese attacked with a state controlled military force with an estimated budget of more than 22 billion dollars a year in today's currency. The terrorists attacked with a small group of non-state actors with an annual budget of around 30 million dollars.[1] Both of these attacks caused the nation and the Army to respond to change.

The events leading up to, and the attack on Pearl Harbor, lead to a declaration of war. The Army grew from an active end-strength of just over 160,000 in 1938, to more than 1.3 million by the end of 1941, and to more than 8 million by the end of the war. The external threat of war and the attack caused the greatest force growth in U.S. History. The terrorist attack of September 2001 caused the Army to change again. This time the theme was not growth but transformation. The centerpiece of Army transformation was the creation of the modular brigade combat team. The Army moved from division centric formations to brigade centric formations in which the necessary enabling forces were assigned to the brigade and no longer task-organized from division controlled battalions. These changes enabled the Army to respond to increased demand for ground combat brigades that was not possible prior to transformation.

Both of these events began with an element of surprise, catching the nation off guard. Both attacks required sophisticated coordination and physical movement of assets that produced collectable indicators. The organizations responsible for providing indicators and warning in both cases failed to provide unambiguous warning to the right

decision makers to counter the attacks. Historical analysis reveals failures in many individual and organizational processes and decisions that led to organizational change across the government. Both events were highly destructive but were relatively discrete events that required great effort by the attacker and carried great risk.

Today, individuals and small groups of people across the globe, operating with inexpensive computers, are involved in cybercriminal activity costing over a trillion dollars a year.[2] These actors do not require the coordination or the movement of physical assets that may produce collectible indicators. Most important, the risk of detection and attribution is very low. This modern threat therefore carries the possibility of large payoff for a small investment and very low risk. In short, it is a great investment, and there is ample evidence that this pressing threat is already inside the wire; exploiting our open society, economy, and military readiness.

The challenge is to design an Army Cyber force that can support the United States Cyber Command (USCYBERCOM) national mission and support operational and tactical formations[3] empowered with the authorities required to defend our interests without infringing on individual freedoms or overly constraining creativity. How should the Army lead and design change to meet the new operating environment? What changes have been made? What is new about the environment? What is the problem we are facing? Who are the stakeholders? What are the solution options?

The Army will conduct further design work to leverage organizations, manpower and operating concepts to fight and win in cyberspace. The Army will accomplish this by integrating emerging doctrine. Army Doctrinal Publication 6.0 (ADP 6.0) on mission command integrates cyber electromagnetic activities as one of the four primary staff

functions. Field Manual 3-38 (FM 3-38) Cyber Electromagnetic Activities (CEMA), currently in draft, details how the army will organize, operate, and integrate cyberspace operations and electronic warfare within the existing warfighting functions. To fully integrate doctrinal concepts, the Army must align functions and missions with the appropriate organizations that contain both offensive and defensive capabilities. This will enable a common operational picture providing coherent situational awareness across the force and allow commanders to synchronize cyber effects. National to tactical integration will occur when the Army mans and trains a cyber educated force across all echelons with the knowledge required to "gain advantage, protect the advantage and place adversaries at a disadvantage"[4] in the cyber maneuver space.

The purpose of this paper is to assess Army efforts to respond to the evolving cyberspace challenges of organizing, manning and operating for decisive operations. The study will use organizational design theory, modeling and approach to describe how the army is adapting to the cyber environment today, discuss current challenges and then make recommendations that will inform how we organize, man and operate forces in a way that moves past individual branch competencies to a synchronized solution on how to fight in the cyber domain.

Background

On June 23, 2009, the Secretary of Defense directed the Commander of U.S. Strategic Command to establish The United States Cyber Command.[5]

USCYBERCOM is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks and when directed, conducts full-spectrum military cyberspace operations (in accordance with all applicable laws and regulations) in order to ensure

U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries.[6]

Army Cyber Command (ARCYBER) is a service element of CYBERCOM. It has two major subordinate commands. 9th Signal Command (Army) “maintains and defends the Network Enterprise to enable information superiority and ensure the operating and generating forces freedom of access to the network in all phases of operations.”[7] The 1st Information Operations Command “provides support to Army commands for planning and execution of Information Operations - also known as IO.”[8]

Army Cyber Command/2nd Army 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 U.S./Allied freedom of action in cyberspace, and to deny the same to our adversaries.[9]

The U.S. Army Intelligence and Security Command (INSCOM) is not a major subordinate command of ARCYBER but has forces under operational control of ARCYBER. INSCOM “conducts intelligence, security and information operations for military commanders and national decision makers.”[10] INSCOM provides intelligence support to ARCYBER activities and currently has the 780th Military Intelligence Brigade (Cyber) as an assigned force. The brigade is under Operational Control of ARCYBER.

9th Signal Command, also known as U.S. Army Network Enterprise Technology Command (NETCOM) “plans, engineers, installs, integrates, protects, defends and operates Army Cyberspace, enabling Mission Command through all phases of Joint, Interagency, Intergovernmental and Multinational operations.”[11]

Military organizations, like their civilian counterparts, require similar components to fulfill their intended purpose. They require structure, people, assets, and other components to accomplish their mission. Military and civilian organizations also require alignment and synchronization of these components to make efficient use of them. Naomi Stanford describes organization design as "the outcome of shaping and aligning all the components of an enterprise towards the achievement of an agreed mission."[12] She also describes five rules of thumb for designing in her book, *A Guide to Organisation Design*:

- "Design when there is a compelling reason.
- Develop options before deciding on design. Will some other interventions other than design be effective? For example: task organization, leader/technical training?
- Choose the right time to design. The current organization still needs to be kept stable and moving.
- Look for clues that things are out of alignment.
- Stay alert to the future."[13]

The compelling reason for further design is the growing threat of malicious cyber activity that affects individuals, private and public organizations, and the military. General Keith Alexander, the CYBERCOM commander, has provided many statements to the public and testimony to Congress about the threat of cyber attacks. In July 2012, in a briefing to the American Enterprise Institute, he stated that he is concerned about when cyber activity "…transition[s] from disruptive to destructive attacks..."[14] He also said the number of cyber attacks on networks is growing. Last year, cyber attacks

increased 44% and malicious software production increased by 60% while attacks on critical U.S. infrastructure went from nine in 2009 to more than 160 in 2011.[15]

The Department of Defense and the Army went through a design process. The most visible result was creation of new structure. The Department of Defense created CYBERCOM and each service created their own cyber commands. The Army has failed to align the remaining components to ensure the new organization functions efficiently, able to accomplish its intended purpose. Naomi Stanford recognizes, “structural decisions usually loom larger in leaders’ minds than other decisions related to organization design…Structure is simply one of the elements to consider…”[16] The military, like many civilian organizations, is enamored with structure.

Historically, most problems found in the land domain were solved by creating new or transformed force structure. If an adversary developed new weapons systems or tactics, the Army could counter with updated organizations, tactics or weapons. The development of the airplane forced land armies to develop their own air forces, air defense weapons, and air defense organizations. The Army could build air defense organizations as organic battalions and operate independently or they could task organize and attach to infantry, armor or field artillery units for protection from air attack. The army has used this process for decades. This is an over simplified example of a complex process but the current process designs force structure that fits the needs of highly structured organizations with built-in service branch hierarchical dependencies.

The cyber threat and domain is not linear, cyber units are not lined up defending on one side and attacking on the other. It is also composed of many actors with different motivations. So far, our response has failed to address these differences. The reason

for this is embedded in our organizational culture; we tend to favor our current process and the results it produces. Jan Kallberg, writing about cyber operations states, “Developments tend to take longer than first anticipated not only because of technological hindrances, but also due to a path-dependent culture favoring earlier methods and natural instinct to prefer what is known.”[17] We need to challenge our assumptions about how we build, align, and assign new organizations. Not every problem demands the same fix. The cyber problem is so dynamic and crosses so many organizational boundaries we need to be comfortable with novel ideas while maintaining a coherent Army unit.

The challenge for the U.S. Military is to develop new organizational structures that achieve the efficiencies and creativity businesses have gained in the virtual and reengineered environments, while at the same time retaining the elements of the traditional, hierarchical, command and control system (for example, discipline, morale, tradition) essential for operations in the combat arena.[18]

Organizing

Currently, ARCYBER pursues two missions in two different locations. First, it operates and defends Army networks through signal units operating under NETCOM and Theater Signal Command direction. Second, it exploits and prepares to attack adversary networks through INSCOM units operating under National Security Agency (NSA) authorities and direction. These functions are separate from one another. Operating units from NETCOM and INSCOM reside in different geographic locations and under their own command and control. Synchronization at ARCYBER takes place three or four echelons removed from the operations. Cyber is still service-centric and

branch-specific. Every service is addressing these problems differently through alignment and command and control changes.[19]

NETCOM signal soldiers are assigned to a signal battalion, which is part of a signal brigade and manning a Theater Network Operations and Security Center (TNOSC). The TNOSC conducts network management and computer network defense of the Army's network in a specific functional theater of operations. The TNOSC also ensures the availability and defense of the Army LandWarNet.[20]

INSCOM conducts signals intelligence (SIGINT) to support Army, other service, and government agency requirements. The INSCOM soldiers conducting SIGINT activities work primarily from NSA operated facilities. The battalion is the basic unit assigned to an INSCOM brigade that conducts operations. The battalions conduct either collection activities or analysis and production. The strategic SIGINT battalions are National Intelligence Program (NIP) funded -- this means NSA provides their military pay. These soldiers work in NSA facilities and receive their day-to-day mission tasking from NSA. Their parent headquarters, the battalion, is assigned to an INSCOM Brigade but is under the operational control of NSA. In the case of a collection battalion, this brigade headquarters is the 704th Military Intelligence (MI) Brigade, located at Fort Meade, MD. For these soldiers and the headquarters, NSA directs their operational activities. The soldiers and headquarters of the analysis and production battalions are assigned to INSCOM brigades that have a regionally aligned mission in support of Theater Armies and work in a cryptologic center. The brigade provides all-source intelligence collection and production in support of the Theater Army commander.

Together, these two types of strategic SIGINT battalions work to support NSA requirements.

NSA requirements come from every part of the government. They support analysis of intelligence problems from the National Security Council (NSC) to tactical units fighting our wars. Over the past decade, NSA has provided expert capabilities to tactical units operating in Iraq and Afghanistan. Army soldiers working inside the NSA provide a unique capability to the agency in supporting tactical requirements. They are well-trained in their SIGINT skills. They also understand Army operations and culture that adds tremendous value to their work.

The Army formed its first army network warfare battalion (ANWB) out of the 704th MI Brigade. The Army manned this unit out of existing SIGINT military occupational specialties (MOS). The Army assigned these soldiers to work in NSA work-centers to conduct cyber activities. The Army has since created the 780th MI Brigade that is commonly known as the “Cyber Brigade.” The ANWB became the 781st MI Battalion and the Army formed a second Battalion, the 782nd, at Fort Gordon, GA. The battalion changed its unit designation and assignment to a new headquarters, but its workforce remains in the same physical location, still directed by the same NSA work-force. The difference is the 780th MI Brigade is currently funded by MI Program (MIP) funds. They are funded by the Army and not NSA. These forces are also under the operational control of ARCYBER, not NSA. In other words, the funding and operational control changed, but NSA still directs it. The Army has a new organization, new mission, and funding, yet the people in the organization still work in the same place with the same supervisors.

The current organization is misaligned. Budget lines of authority for both the Signal and Military Intelligence units conducting the cyber mission originate with the Department of the Army and flow through NETCOM and INSCOM to the operating units. ARCYBER exercises operational control of the battalions on an organizational chart. However, the soldiers in the battalion are executing tasks prioritized by Defense Agencies (DISA and NSA). The parent units (NETCOM and INSCOM) exercise administrative control. The result is that ARCYBER, the headquarters responsible for Army network defense and conducting cyberspace operations, has a near impossible task. The current misalignment ensures that the intelligence soldiers who should be responding directly to ARCYBER tasking and direction still work on tasks prioritized by NSA. The signal soldiers working in the TNOSC still respond to NETCOM and Theater Signal Command priorities.

Part of this misalignment is that the organizations now executing cyber tasks either existed before, or were created before the Army wrote the doctrine and formed ARCYBER. The TNOSC existed before, executing the same missions as it now does. The Army created the 780th MI Brigade as a new organization, but prior to doctrine being written. The Army built the current forms prior to developing the end functional purpose. Jay Galbraith uses an architectural analogy to explain the problem: “When the function and purpose of the end-product is known the design process is started. In architecture, Louis Sullivan’s phrase ‘form follows function’ is commonly used and it is as useful and necessary a precept of organization design as it is for architectural or product design.”[21] The Army needs to take another look at the organization and its alignment to ensure the form (organization) works inside the functions described in the

doctrine. Naomi Stanford follows up by stating, “Sometimes a dilemma for organization designers lies in the question: is the model chosen before the function is known, or is the function determined and then the design model chosen?”[22] Fortunately, the Army created this organization as a Table of Distribution and Allowances (TDA) unit instead of a Table of Organization and Equipment (TOE) unit. This allows changes to individual positions on the authorization document instead of changing entire paragraph numbers—in essence entire teams. The Army can update the existing model through the force management process.

Organizational structure should align budget, mission, direction, and authorities. Proper alignment will achieve unity of command and unity of effort, enabling synchronized defensive and offensive cyber operations controlled and directed by a functional headquarters. The speed of decision required in the cyber domain requires quick, agile decision-making that can only come from unified effort. To this end, the Army should organize and designate ARCYBER as an Army Service Component Command (ASCC) under CYBERCOM. The battalion organizations currently part of NETCOM and INSCOM need to be reorganized and aligned under ARCYBER. The Signal Corps and NETCOM should retain the mission of installing, operating, and maintaining the hardware, software, and physical connections of the network. INSCOM signals intelligence soldiers should still conduct intelligence collection and analysis under NSA authority and direction. The Army should locate the new ARCYBER units at the nexus of the network and intelligence operations in each Theater Army. The Army should assign these ARCYBER battalions to the Theater Army and place them under operational control (OPCON) of ARCYBER. The Army can administer the unit locally

and control operations virtually through CYBERCOM's Joint Operations Center. The specific organization and missions of these organizations will be discussed later as part of operations in this paper.

The description of the organization and alignment of ARCYBER forces above assumes service assignment to the Theater Army. The optimum solution we look for is joint employment of these forces with capabilities to defend, exploit, and attack. The model for these formations already exists. Every cryptologic center in the NSA enterprise has service commanded units working in a joint and interagency environment. The decision to create joint units or service specific units working in a joint environment is dependent on many variables outside the scope of this paper.

Manning

The current workforce in both the Signal and Military Intelligence Corps working in cyber functions is still basic branch controlled. The parent branches manage the soldier's lifecycle. From recruitment to separation from the Army, the Signal and MI enlisted branch managers working with their respective proponent offices have a majority stake in recruitment standards, entry-level training, enlistment bonuses, retention bonuses, assignments, and promotions.

The MI branch and proponent received approval to create the Cryptologic Network Warfare Specialist (35Q MOS) in late 2010. The Army began recruiting for this MOS in 2012. The initial entry training (IET) for this MOS already existed. It was formerly an additional skill identifier course for SIGINT MOS soldiers. The course was previously called the Joint Cyber Analysis Course (JCAC). The course remains unchanged but is now an MOS producing course for the 35Q. The Army reclassified soldiers to the new 35Q MOS who received the JCAC training. The Army assigned the

reclassified soldiers, and will assign the newly recruited soldiers to the 780th MI Brigade. The Army currently has more than 500 authorizations for 35Qs and more than 200 on hand with another 95 in the training pipeline. By the end of 2013, the Army will have more than 300 35Q soldiers in its inventory.[23]

The current manning documents have a standard of grade problem. A healthy MOS should have a pyramid-like structure with more junior enlisted soldiers than mid-grade and senior-grade soldiers. This allows promotions and normal attrition to keep the MOS balanced. The current authorizations for the 35Q MOS are out of balance. There are more senior-grade positions than junior-grade. This will cause quick promotions over the short-term to fill these senior-grades. Once those senior-grade positions are full, promotions will slow down to the point that normal career progression for the MOS will not be possible. Over time this will result in lower morale, job performance, and a loss of a highly skilled workforce to the civilian employment market.

The Army currently uses a model, called in-service recruitment, for other MOSs that it can apply to balance the 35Q MOS and broaden the skill base of its senior members. The model supports manning the existing organizational structure and can scale for individual grade requirements as demand changes. Naomi Stanford recognized that,

Choosing the right model for organization design is one part of the process. The second part is to choose the right approach – the method for initiating the design work but also the way the design will be developed and implemented. The approach must match either the current organizational way of doing things or set the tone for doing things in [the] future.[24]

In-service recruitment is the process by which the Army Human Resources Command (HRC) offers opportunities for soldiers serving in one MOS to re-enlist for another MOS. The basic premise is that some Army jobs require more skilled and mature entry-level soldiers. The Counter Intelligence MOS and the Special Forces MOS are two example programs that recruit from soldiers in service.

The benefits of in-service recruitment for the 35Q MOS are many. It eliminates promotion stagnation by drawing junior enlisted soldiers out of other over-strength MOSs. This allows the MOS to have a more senior grade population with the expert skills required for the mission without having a larger junior-grade force structure than required. HRC can target the in-service program to both MI and Signal soldiers who already possess the technical background skills required. The program also acts as an incentive for high performing individuals in the Army. Branch managers at HRC can set and adjust the requirements for entry to the MOS as needed to maintain a balance between end-strength requirements and supply of qualified applicants. This is more efficiently done with in-service recruiting because all the authorities for this reside internal to HRC. Adjusting requirements for recruiting done in entry-level accessions requires long lead- time and coordination with Army Recruiting Command. The Army also benefits from retaining these soldiers for a longer period of time after training. Entry-level soldiers recruited off the street have less incentive to re-enlist after their first term. They have skills that are in high demand in the civilian marketplace. Soldiers recruited in-service have more time invested in the Army and are more likely to stay in the army until retirement because of time already invested.

Another challenge with the brigade organization is that there are a limited number of locations these soldiers can be assigned. Currently, soldiers are assigned to four locations, although more than 80% of them are assigned to only two locations. This creates challenges for assignment opportunities and exposure to the larger Army. Assignment diversity is necessary for the development of a well-rounded non-commissioned officer corps. Junior-enlisted soldiers promoted to sergeant need to move into leadership positions outside their first unit of assignment to fully develop. Senior NCOs require leadership experiences outside their technical field to prepare them for duties as first sergeants and sergeants major. Structural changes considered earlier in the paper would broaden assignment locations and experience necessary to grow a strong, well rounded NCO corps.

The Signal Corps is in the process of gaining approval for a new cyber MOS, Network Defender (25D MOS). The Signal Corps appears to be using the in-service approach to building their new manning requirements. The proposal has an initial target to convert 414 positions to the new MOS. The proposed structure has 225 staff sergeant, 141 sergeant first class, 40 master sergeant and 8 sergeant major positions. This pyramid-like structure will enable a healthy, balanced population, unlike the current Military Intelligence 35Q structure. The Signal Branch has also proposed a grade and experience career model consistent with the technical capabilities required by duty position and echelon of assignment. The program appears to fit the current requirements for computer network defense requirements and can scale up to meet increased demand from ARCYBER.

The Signal Corps is also creating a cyber related warrant officer career path and a graduate level cyberspace engineering functional area for its officer corps. The new 255S warrant officer MOS and officer Functional Area 26 (FA26) career paths will ensure the Signal Corps builds the required technical and cyber leadership skills required to operate in this new environment.

If we assume both the MI and Signal Corps end with a successful manning model, the next step is to integrate these functions with the mission of ARCYBER. Full integration of these new Signal and MI branch MOSs should lead to discussions about creating a new Cyber Branch. Creation of a new branch and integration is a tough decision because existing branches will lose resources. Naomi Stanford writes it is "particularly challenging in large, mature firms with strong functional groups, extensive specialization, large numbers of people, and multiple, ongoing operating pressures."[25] Both the Signal and MI Corps are large, mature organizations with diverse technical fields. ARCYBER is a new organization. To create the best organization possible, ARCYBER needs to take ownership of its human resources management functions. In the Army this is known as proponency. This will require the creation of a Cyber Branch inside the Army. Again there is an existing model for this; the Special Forces branch at HRC manages all in-service recruiting and personnel management functions for the 18 series MOS. Special Forces branch recruits from soldiers serving in all other MOSs across the Army. It then assesses, selects, trains, and manages the soldiers. A new Cyber Branch will ensure that the organization creates an identity, aligned with its core competencies and mission. Branch identity helps the organization create the esprit de corps necessary in any military organization.

Operating

Combining the functional expertise of the signal and intelligence soldiers will create a workforce capable of executing the ARYCBER mission of planning, coordinating, integrating, synchronizing, directing, conducting network operations, defending all Army networks, and when directed, conducting cyberspace operations in support of full spectrum operations to ensure U.S./Allied freedom of action in cyberspace, and denying the same to our adversaries.[26]

An article in the Signal Corps Army Communicator magazine by Major T.J. O'Conner discussed the need for network defenders to understand how attackers operate. He stated that some officers in his unit were taking classes to gain the expertise to conduct attacks, and that they attended some hacker competitions to gain experience. Through this experience, they discovered that defending Windows XP "is nearly impossible...There is simply no way to patch a decade-old operating system successfully." [27]

Major O'Conner suggests that defenders must know how to attack and what attacker's signatures look like over the network. He suggests that education and experience can close this knowledge gap. Another way to close the gap between individual's expert in defense and in offense is to put them together in the same organization. The Army still keeps the intelligence and signal functions separate in most units today from battalion to echelon above Corps (EAC). There are many past reasons that this occurred over time, but with a new threat and operating environment the organization needs new thinking.

Organization and manning alignment lead to operational effectiveness and efficiency. The Signal Corps still has the requirement to conduct network operations and

the Intelligence Corps still conducts collection activities but the Cyber Corps, freed from these requirements can focus on cyber superiority. The requirement to focus on cyber activities is necessary to be effective because of the speed and episodic nature of contact with the adversary. Jan Kallberg describes “the map and terrain that form the battlespace change continuously in real time and beyond our imagination as new nodes are discovered and a kaleidoscope of network patterns occurs and disappears.”[28]

The most important requirement for effective operations in any domain is situational awareness: the ability to see yourself and your adversary in the same time and space. This is as true of conventional warfare as it is of cyber warfare. The Theater Army or Joint Cyber Operations Center[29] is the new nexus of situational understanding. Inside the commander and workforce share a combined common operational picture of the theater network and the global threat in real-time. The common operational picture is a virtual display of the friendly network, its interaction with the neutral commercial network and the active machine and human malicious actors. Network defenders are monitoring machine logic active defense activities ensuring optimized network performance while recommending human defense activities to counter emerging, or sophisticated threats that can bypass or defeat active machine measures.

Adversary network exploitation soldiers observe the same picture and hunt active threats from human and machine actors. The defenders and exploiters work together passing data in real-time to ensure the friendly network maintains required performance while defeating active threats. Network attack soldiers build on the network defense derived threat capabilities to counter current threats or preemptively strike emerging threats when ordered.

This architecture and situational awareness to gain and maintain cyber superiority does not currently exist. There is no unity of effort in defense and exploitation at the level operations occur. Defense and exploitation operations must be conducted simultaneously and from the same physical location. The situation is similar to developing platforms that combine sensing and shooting capabilities. For example, early unmanned aerial vehicles (UAV) had optical sensing capabilities to locate and identify targets, but depended on another asset to engage. The Air Force added missiles so operators could locate, identify, and engage targets with a single platform. In addition to integrating the sensors with the weapons, we needed to update rules of engagement and authorities to ensure the military conducted targeting in accordance with the law of land warfare. Cyber operators can use the same method. Intelligence operations are bound by public law and executive orders that do not allow intelligence collection on US persons or corporations. Authorities to support private and other non-military public organizations do not exist. The U.S. Congress is still developing legislation that will enable a closer relationship between the military, public, and private enterprise but this is not yet complete. The military has the capability today to execute the first part of the process, which is combining the defense and exploitation capabilities into one organization and location.

An impediment to combining the defense, exploitation, and attack capabilities into one physical location is the classification environment. The Army needs to further align the authorities to operate with the required mission. All signals intelligence work must be done in a Special Compartmented Information Facility (SCIF). Soldiers operating in a SCIF must possess a Top Secret security clearance with access to

certain additional caveats. Soldier must also pass a counter intelligence polygraph to access NSA data. All signals intelligence soldiers meet these requirements but their signal soldier counterparts do not. Both branches need to ensure that soldiers selected for the 35Q and 25D MOS meet SCI eligibility requirements and complete a counter intelligence polygraph. The Army should assign these soldiers to a cyber battalion as discussed earlier in the paper. The Army should organize and assign these battalions according to the requirements of the specific Theater Army and region they will operate in.

The Army will improve offensive and defensive capabilities when it combines the Signal and Intelligence soldiers into the same place by achieving situational awareness. The Army will increase efficiency when it aligns those new organizations under ARCYBER. It will increase the morale, esprit de corps and the retention of the force when it forms a new Cyber Branch. The combination of these changes will lead to further innovation by the workforce as they confront the dynamic challenges associated with this new threat, working together with a common focus.

Challenges

The dynamic nature of the current cyber operating environment makes it difficult for a mature hierarchical organization to respond. The processes we have for design produce forces best suited for 20th century maneuver warfare, where time and physical space are strategic and tactical considerations. The cyber environment is not constrained by physical geography and operates at the speed of light. The current organizational structure, manning, and training are insufficient to operate in this new environment.

- The alignment of unit assignment, budget, authorities to operate and direction are not optimum for ARCYBER to accomplish its mission. The organizations conducting the defense and exploitation/attack are still controlled by the Signal and MI branches working under the direction of defense agencies (DISA and NSA).
- The human resources functions from recruiting, retention, selections, promotions, and separation are controlled by the Signal and MI branches. ARCYBER does not currently act as the proponent.
- There is no unity of effort in conducting the full range of missions ARCYBER is assigned. The organizations conducting the defense of the network and exploitation of adversary networks remain physically separated. There is no situational awareness across those functions.

Recommendations

The Army has the opportunity and imperative to redesign organizations to align the structure, authorities, lines of control, budget, people, and mission of the new ARCYBER headquarters. The Army has several existing models that it can apply to the individual challenges facing it. The challenges will require stakeholder involvement. Signal and MI stakeholders will lose force structure and the money that comes with it. The operating forces of the Army will gain the capabilities necessary to achieve cyber superiority. This study focused on three components of design and makes no claim on having a “correct” solution, only one that will work better than today. The following are specific recommendations that address the broad challenges developed above:

- ARCYBER should become an Army Service Component Command under CYBERCOM.
- Signal and MI forces currently conducting cyber operations should be assigned to ARCYBER.
- ARCYBER should reorganize these forces into multi-functional battalions able to conduct network defense, adversary network exploitation, and prepare to conduct network attack.
- The Army should assign these ARCYBER battalions to Theater Armies and when conditions allow, work in joint and interagency staffed facilities in support of the Combatant Commander.
- ARCYBER should become the proponent for a new cyber branch in the Army and include the 25D and 35Q enlisted MOS, the 255S warrant officer MOS and the FA26 officer functional area, and any other further occupational specialties created working in the cyber field.
- The enlisted cyber MOSs should be approved for in-service recruitment and the authorization documents should reflect only senior grades. The Signal Corps proposal, if approved, is a good model.

The Army should not wait for a surprise attack to cause change. The force growth caused by our entry into World War II or the accelerated transformation caused by the September 11th attack took years to accomplish, yet they were sufficient to meet the challenge. A force growth or transformation to a cyber attack will still take years, but will not be in time to protect the Army and the nation. We cannot wait to respond. We must act now. Fortunately, we have a process and models for other functional

organizations we can use to design a more capable and efficient force, able to operate in this dynamic environment. The Army must not allow the adversary be the catalyst for change, it needs to take the lead.

Endnotes

[1] 9/11 Commission Report.

[2] Information Operations Primer (Carlisle Barracks, PA: U.S. Army War College, November 2011), 23.

[3] COL(P) Chris Ballard, interview conducted at ARCYBER HQs on 10 JAN 12.

[4] U.S. Department of the Army, *Cyberspace Operations Concept Capability Plan 2016-2028*, TRADOC Pamphlet 525-7-8 (Washington, DC: U.S. Department of the Army, February 22, 2010), iii.

[5] United States Strategic Command factsheet, December 2011. http://www.stratcom.mil/factsheets/cyber_command/ (accessed December 31, 2012).

[6] Ibid.

[7] United States Army Cyber Command. http://www.arcyber.army.mil/ (accessed December 31, 2012).

[8] Ibid.

[9] Ibid.

[10] United States Army Intelligence and Security Command. http://www.inscom.army.mil/ (accessed December 28, 2012).

[11] United States Army NETCOM. http://www.army.mil/info/organization/unitsandcommands/commandstructure/netcom/ (accessed December 30, 2012).

[12] Naomi Stanford, *Guide to Organisation Design* (The Economist in association with Profile Books: London, 2007), 4.

[13] Ibid., 12-13.

[14] Bill Gertz, "Cybercom chief: Destructive cyber attacks are coming," July 10, 2012, http://www.beaufortobserver.net/publicationreturnframe.lasso?-token.address=http://freebeacon.com/cyber-war/ (accessed November 12, 2012).

[15] Gertz, "Cybercom chief: Destructive cyber attacks are coming."

[16] Stanford*, Guide to Organisation Design*, 46.

[17] Jan Kallberg and Bhavani Thuraisingham, “Cyber Operations: Bridging from Concept to Cyber Superiority,” *Joint Forces Quarterly*, no. 68 (1st Quarter 2013): 54.

[18] Arthur Huber et. al., The Virtual Combat Air Staff: The Promise of Information Technologies (Santa Monica, CA: RAND, 1996), xiii.

[19] The U.S. Airforce and Navy have moved further toward achieving unity of effort in this regard. Both organizations have combined defensive and offensive units to a degree under the same command and control.

[20] United States Army CIO/G6, http://architecture.army.mil/technical-view/tnosc.html (accessed December 30, 2012).

[21] Jay Galbraith, *Designing Organizations: An Executive Guide to Strategy, Structure, and Process* (San Francisco: Jossey-Bass, 2002), 6.

[22] Stanford, *Guide to Organisation Design*, 33.

[23] SFC Wright, 35Q branch manager, US Army Human Resources Command, phone interview conducted December 12, 2012.

[24] Stanford, *Guide to Organisation Design*, 25.

[25] Ibid., 38.

[26] United States Army Cyber Command. http://www.arcyber.army.mil/ (accessed December 31, 2012).

[27] MAJ T.J. O’Conner et. Al., “Studying Offensive Computing is Esssential,” *Army Communicator* 37, no. 3 (Fall 2012): 15.

[28] Kallberg and Thuraisingham, “Cyber Operations: Bridging from Concept to Cyber Superiority,” 54.

[29] These are notional organizations that do not currently exist. Two organizational models exist that could be used to create a service or joint force capable of executing the cyber mission for a Theater Army or Combatant Commander. NSA cryptologic centers have service provided units OPCON to them working in a joint and interagency environment to conduct the SIGINT mission. DIA also has joint units that support CC Joint Intelligence Operation Centers.