Strategy Research Project

# Off We Go Into the Wild Digital Yonder: Building Cyber Forces

by

Colonel Charles C. Rimbey
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**
Off We Go Into the Wild Digital Yonder:
Building Cyber Forces

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**
Colonel Charles C. Rimbey
United States Army

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
Colonel Darrell Fountain
Department of Distance Education

**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: 6,108

**14. ABSTRACT**

A critical component of the Department of Defense's strategy for operating in cyberspace is the designation of this area of conflict as an operational domain. It is assumed the ensuing organizational change associated with this recognition will more effectively facilitate the organization, training and equipping of forces to dominate our adversaries in cyberspace. These functions, however, remain the purview of the separate military services who also remain the keepers of the profession of arms for their respective domains. Given the increasing importance of the cyber domain, it is time to consider a separate service to ensure the dominance of U.S. Forces in cyberspace. This paper examines the cyber domain beyond the mere designation and takes a more enduring perspective. Current initiatives in cyber command and control are examined but revealed as insufficient in the context of the broader title 10 service responsibilities to organize, train and equip cyber forces. The evolution of the Air Force (from the Army Signal Corps and later the Army Air Corps) is used to validate the evolution to a cyber service.

**15. SUBJECT TERMS**
Title 10, National Security Act of 1947, CYBERCOM, Separate Cyber Service

| **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 | 34 | |

USAWC STRATEGY RESEARCH PROJECT

# Off We Go Into the Wild Digital Yonder: Building Cyber Forces

by

Colonel Charles C. Rimbey
United States Army

Colonel Darrell Fountain
Department of Distance Education
Project Adviser



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

## Abstract

| | |
|---|---|
| Title: | Off We Go Into the Wild<br>Digital Yonder:<br>Building Cyber Forces |
| Report Date: | March 2013 |
| Page Count: | 34 |
| Word Count: | 6,108 |
| Key Terms: | Title 10, National Security Act of 1947, CYBERCOM, Separate Cyber Service |
| Classification: | Unclassified |

A critical component of the Department of Defense's strategy for operating in cyberspace is the designation of this area of conflict as an operational domain. It is assumed the ensuing organizational change associated with this recognition will more effectively facilitate the organization, training and equipping of forces to dominate our adversaries in cyberspace. These functions, however, remain the purview of the separate military services who also remain the keepers of the profession of arms for their respective domains. Given the increasing importance of the cyber domain, it is time to consider a separate service to ensure the dominance of U.S. Forces in cyberspace. This paper examines the cyber domain beyond the mere designation and takes a more enduring perspective. Current initiatives in cyber command and control are examined but revealed as insufficient in the context of the broader title 10 service responsibilities to organize, train and equip cyber forces. The evolution of the Air Force (from the Army Signal Corps and later the Army Air Corps) is used to validate the evolution to a cyber service.

**Off We Go Into the Wild**
**Digital Yonder:**
**Building Cyber Forces**

> The talk you hear...about adapting to change is not only stupid, it's...dangerous. The only way you can manage change is to create it. By the time you catch up to change, the competition is ahead of you.
>
> —Peter Drucker

"The United States is fighting a cyber-war today, and we are losing"[1] according to the former Director of National Intelligence (DNI) and the National Security Agency (NSA) Mike McConnell. Though the definition of what constitutes cyber war remains an item of international negotiation and intense study, there is no doubt we, as a nation, are facing a significant threat in this new area of conflict. Evidence is provided almost daily in the media. Hackers in Chinese Cyber Unit 61398 have stolen "technology blueprints, negotiating strategies and manufacturing processes from more than 100 mainly American companies"[2] as reported by the highly respected American cyber security company Mandiant. A related *New York Times* investigation found that hackers targeted a cyber security company supporting American intelligence organizations as well as American defense contractors and even compromised the networks of a company supporting the operation of American power grids and pipe lines[3]. Former Secretary of Defense, Leon Panetta, warned of a cyber Pearl Harbor that "could endanger the U.S. power grid, transportation network and financial services.[4] Clearly, the cyber threat to our nation is real, growing and warrants decisive action to ensure our military forces are ready for the challenge.

In response to this looming threat, the U.S. Government is vigorously studying, debating, and to some extent developing a holistic governmental approach to

cyberspace. The Department of Defense's (DOD) response has been primarily focused on command and control (C2) of cyber forces and networks, and in this realm, important, incremental steps have been taken. A major step was the 2010 creation of the United States Cyber Command (CYBERCOM) as a sub-unified command under the United States Strategic Command (STRATCOM) 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.**[5] (emphasis included in original)

Assigned to CYBERCOM, each service has further established a service component command: Army Cyber for the Army, Marine Cyber for the Marines, the 24th Air Force for the Air Force and the 24th Fleet for the Navy.

With its new charter, CYBERCOM is currently undertaking multiple key initiatives. The command is developing standardized training packages that can be delivered to the services. These packages are designed to ensure that all cyber professionals have at least a minimum standard set of tools required to enable their duty performance. The command is also developing standardized force packages, Cyber Support Elements (CSEs), that consist of an integrated group of cyber professionals with varying skill sets, some offensive, some defensive, which can be provided to supported organizations--primarily Geographic Combatant Commands. As GEN Keith Alexander testified before the senate on March 12, 2013, "...we are already developing the teams that we need, the tactics, techniques and procedures, and the doctrine for how these teams would be employed."[6]

However, according to a recent study by the Defense Science Board, DOD's efforts "though numerous, remain fragmented" leaving DOD "not prepared to defend against this threat."[7] One of the Board's primary recommendations is that USCYBERCOM, and its supporting Service Component Commands, "must be the driving force to surface the doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) /Unity-of-Effort gaps and advocate for requisite gap-closure actions."[8] These gaps are to be addressed by the separate military services, however each service will undoubtedly choose to address them in the context of and for the good of their service equities. Without central controlling focus, the four services are doing what they feel is best for their services rather than following a coherent strategy dedicated to dominance in the cyber domain.

CYBERCOM, the recognized sub-unified command created to execute C2 of cyber forces, is organizing, training and equipping cyber units for the execution of cyber operations. They are doing so out of necessity but they are not the appropriate organization to accomplish these tasks that are, by law, accorded to the services, not combatant commands. It cannot be assumed that the ensuing organizational change, associated with the creation of the operational domain of cyber and the advent of CYBERCOM, will effectively facilitate the adequate organization, training and equipping of cyber forces to dominate our adversaries. What is needed is a separate cyber-focused service to coherently and without bias, man, train, and equip cyber forces and then, as dictated by Goldwater Nichols, turn them over to CYBERCOM for the execution of cyber missions. The DOD need only look to its own history for the justification of this solution. The evolution of the Air Force (from the Army Signal Corps and later the Army

Air Corps) offers an effective example of how the realization, incorporation and inculcation of a new set of technologies can be appropriately addressed.

## Origins of the Services and Roles / Functions of DOD Organizations

The initial Services of the United States Armed forces, the Army and the Navy, were established in 1775 and were first codified in the US constitution, ratified in 1787. By the time the United States was established in 1776 it was readily apparent that although we lived on the land, we depended on ready access to the global commons of the sea to allow trade and commerce with other nations. Hence, in establishing the original version of the US armed forces the framers of the constitution gave the United States Congress the power to "raise and support Armies"[9] as well as "provide and maintain a Navy."[10] Today, the responsibilities of the different elements within DOD are codified in Title 10 of United States Code. Under Title 10, there are three military departments: The Department of the Army, the Department of the Navy and the Department of the Air Force.[11] The secretaries of each of the three departments are charged with:

> … recruiting, organizing, supplying, equipping (including research and development) and training,"[12] and "carrying out the functions of the department…so as to fulfill the current and future operational requirements of the unified and specified combatant commands[13].

"It is the task of each military department to perform all the management functions—from initiating research to issuing operational weapons, from recruiting men to procuring and transporting materials—all addressed specifically to enable the military commander to fight most effectively"[14]. Normally these broad duties are simplified to man, train and equip.

Further, each of the three departments is directed by law to provide forces focused on a specific domain. The Army "includes land combat and service forces and such aviation and water transport as may be organic therein. It shall be organized, trained, and equipped primarily for prompt and sustained combat incident to operations on land. It is responsible for the preparation of land forces necessary for the effective prosecution of war."[15] The Navy "includes, in general, naval combat and service forces and such aviation as may be organic therein. The Navy shall be organized, trained, and equipped primarily for prompt and sustained combat incident to operations at sea. It is responsible for the preparation of naval forces necessary for the effective prosecution of war."[16] The Air Force "includes aviation forces both combat and service not otherwise assigned. It shall be organized, trained, and equipped primarily for prompt and sustained offensive and defensive air operations. It is responsible for the preparation of the air forces necessary for the effective prosecution of war."[17] Each of the services is clearly focused on a domain of warfare so as to enable mastery of the domain and ensure U.S. dominance during times of conflict.

A study on combining services by the U.S. Naval institute in 1961 determined separate services for mastery of the land, sea and air are necessary to provide the "knowledge of the principles and doctrine of a particular kind of warfare which can only be gained from constant study and training and practice and dogged effort."[18] The study further asserted, "Much of the successful prosecution of war which our fighting forces have achieved has been due to the determination of each military service to develop the art of warfare for which it is responsible to the highest degree of effectiveness and to the concentration of each military department to support and enhance its service in carrying

out that function."[19] Clearly separate services are required to develop the unique implements of war for the domination of land, sea and air.

Though title 10 services provide manned, trained and equipped forces, the Goldwater Nichols Act of 1986 dictates the joint command and control environment in which combatant commanders conduct operations. The title 10 functions of combatant commanders include:

> …giving authoritative direction to subordinate commands and forces necessary to carry out missions assigned to the command including authoritative direction over all aspects of military operations, joint training, and logistics; prescribing the chain of command to the commands and forces within the command; organizing… (and) employing forces within that command as he considers necessary to carry out missions assigned to the command [20]

Notice that although functions such as training and organization are addressed, they are addressed only as necessary to carry out the command's specific missions. The combatant commander wields the tools that the domain-focused military departments provide; binding the service provided units together into a coherent joint force.

## The Fifth Domain (Cyber)

Often referred to as the fifth domain, after earth, sea, air and space, the first tranche of what has come to be known as cyberspace was initially conceived by the military as a means for linking computers at multiple universities to allow collaboration on DOD funded projects. This connectivity was established to enhance reliability, survivability and productivity of key computing operations. It exists today as a vastly expanded almost ubiquitous nodal network abstraction that is both distinct from the physical domains in which it resides and dependent on them. The tremendous power that this nodal network fabric affords our modern society has caused our nation, and by

extension our military forces, to increasingly depend on the cyber domain to connect key sensors, shooters, and enhanced capabilities in all other physical domains.

The cyber domain, while a logical abstraction, has real effects, both beneficial and detrimental, upon the very domains on which it depends for existence. From the accidental destruction of turbines at a Russian dam[21] due to an operator's mistake, to the very purposeful destruction of Iranian centrifuges by STUXNET,[22] there can be no doubt that cyber activities can have kinetic, destructive effects on objects in the physical domains. The battlefield now includes anywhere a device is connected to a network. This extension of the battlefield, due to the introduction of a new technology, is not unique. Barely two decades after the first manned heavier than air flight at Kitty Hawk, theorist B.H Liddell Hart wrote "A nation's nervous system is no longer covered by the flesh of its troops".[23] This was a response to the expansion of warfare beyond the battlefield created by the introduction of strategic bombing. Additionally, H.G. Wells prophetically wrote of the air domain in 1907,"…in the air [there] are no streets, no channels…In the air all directions lead everywhere."[24] Correspondingly, in the cyber domain, national boarders are crossed by beneficial, innocuous as well as nefarious bytes of data with relative impunity in the blink of an eye.

In the cyber domain, dimensions such as time and space are given new meaning and context. Human beings that intuitively understand how to effectively operate militarily in the world of physical, geographic domains, find themselves perplexed by the abstraction of the cyber domain[25]. Our understanding fails us in a domain where, "Weapons can be reproduced instantly, bullets travel at near the speed of light, destroyed targets can be brought back from the dead, and a seventeen year old can

command an army"[26]. This critical, essential but vastly different domain requires a specialized approach--a different way of operating and most importantly of thinking from the other domains that are the purview of the four extant services. The history of the United States Air Force, offers an example of how both the Armed Services and the nation, dealt with a similar situation; the advent of the air domain.

## In Search of Domain Mastery, a Case Study

Though the Air Force recognizes its birthday as September 18, 1947, the date of the Defense Authorization Act of 1947, it did not spring, fully formed into being on that day. Instead it grew into a separate service through an evolving recognition of the unique Title 10 service activities required to master this new dimension of warfare. From the very beginning, it was clear that this new domain demanded a level of focus and dedicated study that the US Army Signal Corps was ill prepared and reluctant to provide.

On 1 August, 1907, BG James Allen, convinced of the potential of aviation by MAJ George O. Squier and his assistant, CPT William "Billy" Mitchell, issued a memorandum establishing the Aeronautical Division of the Office of the Chief of Signal that was in charge of "of all matters pertaining to military ballooning, air machines, and all kindred subjects"[27]. This first precursor to the modern day air force, although small (3 men), allowed a separate entity, unencumbered by land-based or signal duties, to focus on the advancement of this separate domain and it's utility to warfare. It was this organization that nurtured the research and development of aerial warfare and led to the acquisition of the military's first airplane, purchased from William and Orville Wright, on August 2, 1909 for $30K[28] ($750K in 2013 dollars). Interestingly, this is the same amount that was appropriated to the Army for the development and purchase of a

technology more prominent in the Signal Corps--wireless telephone equipment.[29] The Aeronautical Division, a separate administrative directorate, focused solely on the development of technologies and doctrine in this new domain. Without it, the mastery of the air for military purposes would have lagged significantly behind that of our future adversaries leading into the crucial years immediately preceding World War I.

However prior to 1911,devoid of a strong voice at a high enough level to advocate for funds from congress and a "marked lack of enthusiasm for aeronautics among many of the Army's line officers"[30], the Signal Corps struggled to maintain its fledgling aviation program. Congressional lack of enthusiasm was typified by the Congressman who reportedly asked "Why all the fuss about airplanes for the Army? I thought we already had one."[31] With no appropriated funds, the Signal Corps was forced to maintain their aircraft out of general funds intended for other, more recognized efforts such military telephone and telegraph installations[32]. For example, in 1910 there was only $150 available for fuel and repairs[33] (what would today be considered O&M costs). Additional resourcing challenges faced by Army Aeronautics, including reliance on borrowed officers begrudgingly provided by numerous branches. Officers were exceedingly hesitant to be a part of this new effort. Their concern "stemmed from the lack of a clearly defined status and function for aviation within the service."[34] Due to resource constraints, it was increasingly difficult for the Signal Corps to execute aviation training without detriment to their other core missions.[35] However, legislation introduced in 1913 by Representative Hay to establish aviation as a separate branch from the Signal Corps received little support (though Hay was Chairman of the powerful Military Affairs Committee).[36] Even William, "Billy" Mitchell, who was eventually court martialed

for his ardent support of a separate service, along with most military aviators at the time, opposed the bill because "aviation had not developed to the point of becoming a separate arm or service."[37] Soon after, however, Congress finally passed legislation creating the Aeronautical Section of the Signal Corps, a more permanent and higher standing organization consisting of 60 officers and 260 enlisted men,[38] headed by then Major Billy Mitchell.

In the area of leadership, although some element of permanence and stability had been established, military aviators increasingly expressed dissatisfaction with the non-aviator officers commanding them. The consensus was that the non-aviators who flew rarely or not at all could not understand "the limits of the airplane, the importance of maintenance, or other considerations affecting flight safety."[39] These feelings continued to grow "eventually becoming a major factor in the gradual attainment of autonomy of the air arm."[40]

It was also during these early years of military aviation, that the lack of standardized training hindered development of the profession of arms in the air domain. Some potential aviators, including the likes of Henry H. "Hap" Arnold learned the basics of flying at the factory school run by the Wright brother's in Dayton, Ohio, while others were sent to the Curtiss factory in San Diego.[41] The resultant pilots' disparate skill sets contributed significantly to the American air arm's uneven initial performance during World War I. Additionally, there was no central school for the study of air doctrine hindering the development this new dimension of the profession of arms.

Following the end of World War I there was much debate and discussion on the organization of the post-war military's air arm. Many of our wartime allies, including

Great Britain, had established separate air forces during the war and proposals by congressmen and even a War Department board recommended a separate Department of Avionics[42]. The National Defense Act of 1920 officially established the Air Service as a combatant Arm of the Army, equivalent in stature to other long-established arms such as its progenitor the Signal Corps as well as the infantry and armor. This organization was given the permanent assignment of a complement of men as well as a major general as its chief and a brigadier general as his deputy[43]. Unlike the other combat arms of the Army, the Chief of the Air Services was given control over procurement of aircraft, research and development in aviation, as well as the recruitment and training of aviation personnel[44]. Additionally, addressing prevailing concerns over the air leadership's technical competence, the act specified that only aviators would command flying units and that non-aviators would be limited to no more than 10 percent of the service staff[45]. Overall, this act "ensured unified control of the most important aspects of the air mission"[46] finally providing the Army's air arm the authorities it needed to man, train and equip air focused organizations

It is important to note that at this point in the development of America's Armed Forces, the Department of Defense had not yet been established as a central overseer of the military services. This was also before the Goldwater Nichols act of 1986, emphasizing joint command of military forces, eliminated the services' command and control of operational forces. The Defense Act of 1920 fixed all air related service responsibilities, with the exception of budget, upon the Army Air Service. The Army, in the guise of the War Department, only maintained control of the C2 aspects of the mission. This is in fact the opposite of the situation today where C2 of the cyber

operational mission has been delegated to CYBERCOM, while the service related, Title 10 responsibilities related to cyber, are still distributed, or more precisely fragmented amongst the services.

During the balance of the interwar years, aviation supporters, such as Mitchell, continued their campaign both in the government and the public, on the utility of air power and its ability to execute missions beyond the support of ground or naval forces. However, it would take the demonstrated offensive capabilities of strategic bombing forces in a second world war, as well as the advent of the ultimate strategic weapon, the atomic bomb, to convince leaders in the Government of the necessity of a completely separate service. The Chief of Staff of the Army, GEN Dwight D. Eisenhower typified the prevailing sentiment testifying that a separate Air Force was "so logical from all our experience in this war—such an inescapable conclusion—that I for one can't even entertain any longer any doubt to its wisdom."[47] Immediately after he signed the National Security Act of 1947, establishing a separate Air Force as well as a Secretary of Defense, President Truman issued Executive Order 9877, "Functions of the Armed Forces" making each of the three services "responsible for the medium—air, ground, or sea—in which it operated"[48] Finally, forty years after the Wright brother's first flight, the United States had a separate, autonomous service dedicated to manning, training, equipping and leading forces in the technically dominated air domain.

## Manning Cyber Organizations

When asked the biggest challenge CYBERCOM currently faced, during his congressional testimony in September 2010, CYBERCOM's commander, GEN Alexander, stated, "it's generating the people that we need to do this mission."[49] Given the significance of this challenge we should not ask the Combatant commands to

simultaneously recruit, train and organize cyber warriors into fighting units. These functions are beyond their charge. Similarly, CYBERCOM ought not perform these inherently Title 10 service-oriented tasks while they are defending the United States against cyber attack.

GEN Alexander wrote that CYBERCOM's "mission document states that we coordinate, integrate, and synchronize activities to direct the operations and defense of DOD Networks,[50]" indicating an operational, real world, 24 hour a day mission. This does not include recruiting and building the workforce and the tools they utilize. Also according to GEN Alexander "We are reviewing recruitment and incentive programs in order to build and retain the best of the best cyber defenders, and we are working to standardize, track, and manage the training needed for all cyber personnel."[51] These are again title 10 tasks normally associated with a service not a Combatant Command.

This point is also further validated in USCYBERCOM's Concept of Operations, released in 2010, which states that

> the services retain primary responsibility to man, train, and equip for mission readiness, administration, and management of those forces under the command and control of U.S. Cyber Command. The Concept of Operations directs the service components assigned to U.S. Cyber Command to develop capabilities in support of operational requirements from U.S. Cyber Command[52].

In this same study "service officials expressed concern that if offensive cyberspace operations require greater personnel resources, competing demands from other mission areas may make it difficult for the services to provide additional military personnel in support of U.S. Cyber Command's activities."[53]" This harkens back directly to the early American air arm's inability to acquire the personnel required to build air power.

Meanwhile, the Department of Defense declared, in its Quadrennial Roles and Missions Report of January 2009 that it had "decided to develop a professional cyberspace force able to influence and execute cyberspace operations with the same rigor and confidence as traditional Department operations in other domains.[54]" Therefore, in essence, DOD is declaring it will execute operations in cyber as in the other domains while the services, who's mission it is to master those domains, are concerned with competing demands within their own areas of expertise. These more organic service demands will invariably hamper the service's ability to vigorously support cyber. Again these conditions parallel the evolution of the Air Force as a service.

## Training Cyber Warriors

On January 27, 2013 the *New York Times* announced that the Defense Department was seeking to more than quadruple its "Cyber Security Force" adding more than 4000 "world class cyber personnel."[55] It will be essential that these newly recruited service men and women are provided a standardized training program. When asked, during congressional testimony, how CYBERCOM will improve "the department's ability to provide a trained cyber force,"[56] GEN Alexander replied, "whether it's the tools we create or the students we put through there -- doing it as a joint force with one standard is the key thing."[57] However, as verified in GAO reports, "The services have started to develop their own cyber training programs geared toward service-specific cyberspace requirements."[58] For example, the Army and Navy are utilizing the Joint Cyber Analysis Course, run by the Navy, while the Air Force has established its own

training courses[59]. Without central controlling direction, the separate services are developing training programs focused on each services' unique domain perspective.

## Equipping Cyber Forces

The equipping of cyber forces remains just as important an area as that of the other kinetic effects based forces. The tools of a cyber warrior are not the hardware that builds the domain but the software that establishes it, or in the case of offensive cyber operations, attacks its linkages and functions. Though much of the development is classified, one may assume that the development of highly precise software "weapons" is a highly complex acquisition. Unconfirmed reports estimate that the STUXNET virus took "at least three years to develop…at a cost in the double-digit millions."[60] The acquisition and R&D processes are also the Title 10 responsibilities of the services. Just as in manning and training, it takes a service focused on those processes, as well as ardently advocating for the monetary resources to support them, to truly develop the precision arsenal that operations in cyberspace demands. Recall that the acquisition and R&D of aircraft were the first authorities transferred to the Army's air arm.

## Leading Cyber Forces

Although not normally mentioned as part of the man, train, and equip duties of military services, leadership is none-the-less key. One of the primary arguments for a separate, independent air force was the perceived need for leadership by officers trained and experienced in the new form of warfare the air domain required. Italian General, Giulio Douhet, one of the major early air power theorists, realized by 1914, just six years after his nation's first aircraft had flown and even as his armed forces were still focused on dirigibles, "that the aircraft could become a dominant weapon only if it were

freed from the fetters of ground commanders who did not understand this new invention"[61]. His thoughts were later echoed by the American advocate of a separate Air Force, Billy Mitchell, who testified before the Morrow board in 1925 that, "In every instance of which I have known or heard the result of placing other than air officers in charge of air power has ended in failure."[62]

Correspondingly, in their article "Leadership of Cyber Warriors: Enduring Principles and New Directions" Colonels Conti and Raymond contend that successfully leading cyber warriors takes a different type of leader. They assert that this cyber dominance requires one who is "comfortable in this new inherently technical and abstract domain, appreciates technical expertise, and understands the personality types, creativity, culture, motivations, and intellectual capability of cyber warriors." Thinking and leading in cyber requires a different perspective from those who thrive in the kinetic domains. Comments from non-cyber leaders in cyber organizations such as, "Marines assigned to MARFORCYBER will still be riflemen first and not Hollywood-style 'geeks' with only computer skills… while there will be some associated skills for cyber, they will remain Marines first, cyber warriors second,"[63] demonstrate the lack of appreciation for the differences inherent in cyber operations and the highly technical personnel required to run them.

## Recommendations

During congressional testimony GEN Alexander emphasized, "What we don't want to do is say, well, the Navy will do Navy and the Army will do Army and the Air Force will do Air Force"[64]. However, service centric solutions are invariably going to be the norm when each service is developing its own version of cyber forces. The DOD needs consistency, not just in command and control of operational cyber forces, but in

the strategy of how we man, equip, train and lead these valuable resources. It is clear that though DOD has made significant strides in the coherency of cyber C2, we have been far less successful in the development and standardization of the tools to be commanded and controlled. This is the area that Title 10 would normally direct a service to accomplish but history has shown us that the development of new forces within a service is problematic. Developmental efforts that are not the primary focus of a given service often lack direction, focus and most critically, resourcing. Services will, by nature, focus their resources on what they deem are the essential tools required to dominate their domains. The Army will always focus on tanks, the Air Force on fighter aircraft, the Navy on aircraft carrier groups. The best way to remedy this situation is to learn from history and match the changes we have made in the C2 of cyber forces with equally substantial changes to the organizations that provide them. This can only be accomplished by establishing a separate Cyber Service to function as the Title 10 entity that mans, organizes, trains and equips the world's preeminent cyber force.

A Separate Cyber Service

Establishing a separate military service for cyber would demonstrate the ultimate recognition of the true significance of the cyber domain to our nation's defense. Only a separate service to man, train and equip cyber forces can effectively, coherently and comprehensively address the challenges cyberspace presents. This is not to say that there will not still be a requirement for cyber skilled individuals in the current services. Even after the 1947 separation of Air Force from the Army, there were still aviators required in each of the other domains. Correspondingly, there will still be a requirement for cyber personnel in each service to execute tasks that are peculiar to those other services, mainly at the tactical level. However, as cyber forces continue to evolve,

particularly those focused on offensive and exploitive operations (analogous to strategic bombers) they will be able to operate independently of the other domains with the potential of achieving diverse and increasingly precise and devastating effects on potential targets. And as foreseen by Douhet, strategic bombers and nuclear weapons opened up the aperture of what could be attacked directly, without fighting through a ground army or maritime force. The cyber domain similarly allows military targets to be engaged with new and abstract concepts separate, distinct and foreign to our existing services.

Just as the nation determined through the development of the Air Force, a new, focused organization is required to address a new domain. The only way to truly develop the capable forces needed to dominate a new domain without unnecessarily burdening operational commands is to establish a separate, Title 10 service responsible for manning, training and equipping those uniquely capable forces. There may, however, be some fear and trepidation associated with establishing a separate service, particularly given the resources required. However, a separate cyber service doesn't have to look like the other services, just as members of that service may not look like members of the other services. The service just needs to have the people it requires to perform the requisite Title 10 functions. Further, there can still be a sharing rather than duplication of resources. When the Air Force was finally created in 1947, they continued to share the primary quartermaster supply of common items such as uniforms.

But much as in the evolution of the United States' air arm, the establishment of a Cyber Service is a sweeping step that many in our government are hesitant to take.

However, as a nation, we should not wait until there is some cataclysmic populace-affecting cyber event as in the past when Pearl Harbor and 9/11 were the stimulus required for the creation of NSA and DHS respectively[65]. A potential intermediary step we can take immediately is the employment of a model based on the service-like Title 10 functions bestowed upon SOCOM.

USSOCOM Model

The US SOCOM model has been advocated in numerous papers, articles and discussions as a model for C2 of Cyber Forces[66]. However, the model is also apropos as an incremental step towards the manning, equipping and training of cyber organizations. According to Title 10, US Code, beyond the authorities granted to every other Combatant Commander, the USSOCOM commander "is responsible for, and has the authority necessary to conduct…all affairs of such command relating to special operations activities, including: In coordination with the Military Service Chiefs, organize, train, equip, and provide SOF, doctrine, procedures, and equipment"[67] (including research and development and operational testing). These are title 10 functions normally granted exclusively to the military services. A similar set of authorities would give CYBERCOM the mandate it needs to direct the correction of the primary sourcing deficiencies identified in manning, equipping, and training the force, akin to the direction provided by the US Army Air Corps in 1926.

Military services must still, however, maintain separate training and equipping models for their special forces because their operators are based in, and need to still maintain expertise in, their respective domains of dominance. Though they can and frequently do, operate across domains, their primary raison d'être, as a separate special force entity is their domain of origin. Seals are "maritime warriors", Rangers "conduct

airborne and air assault operations…in squad through regimental operations" and the Air Force Special Ops are "America's specialized air power"[68]

However Cyber, the first man-made domain, although physically resident in the other domains in the form of facilitating infrastructure, displays a unique, abstract and consistent set of characteristics as it traverses and exists amongst the land, sea and air. In many respects, it is consistent across its entire width and breath and therefore requires a different way of thinking. The first chief of staff for Marine Cyber Command, COL Steve Zotti, put it this way: "One of the challenges is that cyber, by its very nature, is a global domain, so you need some level of standardization, but also the ability to tailor TTPs [tactics, techniques, and procedures] to specific regions and threats, although traditional boundaries do not necessarily apply."[69] The emphasis is on standardization and tailored TTPs based on differences in the region or the threat being countered, not the domain or the service that is providing the forces.

Although the SOCOM model could be an admirable evolutionary step in the right direction, it remains insufficient to adequately address the challenges of building cyber forces. Allowing each service to continue building their own versions of cyber capabilities will only exacerbate the fight for resources--personnel, equipment and dollars, in an already fiscally constrained environment. Further, there is a great potential for needless and potentially detrimental duplication of efforts. Finally, the scope of building forces while simultaneously directing the execution of cyber operations is simply too much for one headquarters to handle effectively. Only the establishment of a separate cyber service dedicated to building cyber forces will be able to provide DOD

the professionally manned, trained and equipped forces it needs to the lead in the cyber domain.

## Conclusion

In his 1921 seminal treatise on the use of airpower, “The Command of the Air” Douhet wrote “victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur.[70]” From power meters to electric cars[71], as more and more devices, are connected to the cyber domain, that domain ever more closely resembles the ubiquitous air of which Mitchell likened to “a fluid that covers the whole earth like a deep blanket."[72] It is clear we are on the cusp of a new type of warfare, the magnitude of which we are just beginning to realize in a domain we struggle to comprehend.

Though a chorus of leaders in DOD and government proclaim that the cyber domain, and operations within it, are critical to both the military and the country, only a few, if any, truly comprehend the ramifications of cyberspace. Cyberspace and cyber operations demand the sole focus of an organization filled with of our best and brightest service men and women and professional leaders to give them direction. Command of cyberspace, just as Douhet’s “Command of the Air” can only be attained with a professionally manned, trained and equipped Cyber Force. And as our farsighted forefathers stipulated the maintenance of a technically competent Navy to vigilantly patrol our colonial seas, and the greatest generation insisted on a technologically superior Air Force to rule the cold war skies, it is time for our nation to create the change that keeps us ahead of our competition. We must create a cyber service that ensures we have the world’s foremost cyber force to dominate the new frontiers of cyberspace.

## Endnotes

[1] Mike McConnell, “Mike McConnell on How to Win the Cyber-War We're Losing”, *The Washington Post*, February 28, 2013.

[2] “China’s Cyber-Hacking, Getting Ugly”, The Economist, February 23-March 1, 2013, 12.

[3] Ibid.

[4] Elisabeth Bumiller and Thom Shanker, “Panetta Warns of Dire Threat of Cyberattack on U.S.”, *New York Times*, October 11 2012.

[5] BG George Franz, “CYBERCOM” briefing slides with scripted commentary, Carlisle Barracks, PA, U.S. Army War College, December 18, 2012, Slide 2.

[6] GEN Keith Alexander, House Armed Services Subcommittee, Cyberspace Operations Testimony, Washington D.C., March 12, 2013.

[7] Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat*, (Washington DC: US Government Printing Office, January 2013), 1.

[8] Defense Science Board, Resilient *Military Systems and the Advanced Cyber Threat*, 51.

[9] US Constitution, Article 1 Section 8

[10] Ibid.

[11] USCODE Title 10-Armed Forces (2011),17 section 101 (a)(8).

[12] USCODE Title 10-Armed Forces (2011), 1821 section 3011 (a)(2)(b).

[13] USCODE Title 10-Armed Forces (2011), 1821 section 3011 (a)(2)(c).

[14] US Naval Institute, *The Reorganization of the Department of Defense, Philosophy and Counter-Philosophy*, (Annapolis Maryland, U.S. Naval Institute, 1961) 21.

[15] USCODE Title 10-Armed Forces (2011), 1821 section 3062 (b).

[16] USCODE Title 10-Armed Forces (2011), 1821 section 5062 (b).

[17] USCODE Title 10-Armed Forces (2011), 1821 section 8062 (c).

[18] US Naval Institute, *The Reorganization of the Department of Defense, Philosophy and Counter-Philosophy*, 21.

[19] Ibid.

[20] USCODE Title 10-Armed Forces (2011), 17 section 101 (c)(1)(A-F)

[21] On August 17, 2009, a technician at Sayano-Shushenskaya hydroelectric dam in Russia mistakenly remotely started a 10 ton turbine that had been shut down due to excessive vibration. The resulting accident as the turbine vibrated off its pad killed 75 people and injured many more. Additionally, 40 tons of oil were spilled in the Yenisei river. Joe P Hasler, "Investigating Russia's Biggest Dam Explosion: What Went Wrong" *Popular Mechanics Online* (February 2, 2010) Investigating Russia's Biggest Dam Explosion: What Went Wrong - Popular Mechanics (accessed March 13, 2013).

[22] In "the first known digital attack launched by a government to destroy another country's physical infrastructure", 1000 of Iran's 5,000 enrichment centrifuges were temporarily put out of commission by the malware, and some sources within the Obama administration told the Times that Iran's nuclear ambitions may have been set back by as much as 18 months to two years. Andy Greenberg, "What Stuxnet's Exposure As An American Weapon Means for Cyberwar", *Forbes Magazine Online*, (June 1, 2012), http://www.forbes.com/sites/andygreenberg/2012/06/01/what-stuxnets-exposure-as-an-american-weapon-means-for-cyberwar/ (accessed March 13, 2013).

[23] Capt Basil H. Liddell Hart, *Paris, or the Future of War* (New York, NY: Global Publishers, 1972 [cl925]), 36-37.

[24] H.G. Wells,*The War in the Air* (London, U.K, George Bell and Sons, 1908), 247.

[25] Matthew Miller, Jon Brickey and Gregory Conti, "Why Your Intuition About Cyber Warfare is Probably Wrong", *Small Wars Journal Online* http://smallwarsjournal.com/jrnl/art/why-your-intuition-about-cyber-warfare-is-probably-wrong (November 29, 2012).

[26] Ibid.

[27] Rebecca Robins Raines, *Getting the Message Through, a Branch History of the US Army Signal Corps* (Washington D.C.: Center of Military History, United States Army, 1952) 127.

[28] William C. Heimdahl and Alfred F. Hurley, "The Roots of U.S. Military Aviation," in *Winged Shield, Winged Sword: A History of the United States Air Force* Vol. I, ed. Bernard C. Nalty, (Washington D.C., United States Air Force,1997), 14.

[29] Robins Raines, *Getting the Message Through, a Branch History of the US Army Signal Corps,* 139.

[30] Alfred Goldberg, *A History of the United States Air Force 1907-1957* (Princeton, NJ: D. Van Nostrand Company, INC, 1957), 6

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Heimdahl and Hurley, "The Roots of U.S. Military Aviation," in *Winged Shield, Winged Sword: A History of the United States Air Force* Vol. I, ed. Bernard C. Nalty, 27.

[35] Ibid.

[36] Heimdahl and Hurley, "The Roots of U.S. Military Aviation," in *Winged Shield, Winged Sword: A History of the United States Air Force* Vol. I, ed. Bernard C. Nalty, 27-28

[37] Goldberg, *A History of the United States Air Force 1907-1957*, 8

[38] Heimdahl and Hurley, "The Roots of U.S. Military Aviation," in *Winged Shield, Winged Sword: A History of the United States Air Force* Vol. I, ed. Bernard C. Nalty, 28

[39] Heimdahl and Hurley, "The Roots of U.S. Military Aviation," in *Winged Shield, Winged Sword: A History of the United States Air Force* Vol. I, ed. Bernard C. Nalty, 29

[40] Goldberg, *A History of the United States Air Force 1907-1957*, 7

[41] Heimdahl and Hurley, "The Roots of U.S. Military Aviation," in *Winged Shield, Winged Sword: A History of the United States Air Force* Vol. I, ed. Bernard C. Nalty, 20

[42] Goldberg, *A History of the United States Air Force 1907-1957*, 29

[43] John F. Shiner, "From Air Service to Air Corps: The Era of Billy Mitchell," in *Winged Shield, Winged Sword: A History of the United States Air Force* Vol. I, ed. Bernard C. Nalty, (Washington D.C., United States Air Force,1997), 76.

[44] Ibid.

[45] Shiner, "From Air Service to Air Corps: The Era of Billy Mitchell," in *Winged Shield, Winged Sword: A History of the United States Air Force* Vol. I, ed. Bernard C. Nalty, 77

[46] Goldberg, *A History of the United States Air Force 1907-1957*, 29

[47] Herman S. Wolk, "From Air Service to Air Corps: The Era of Billy Mitchell," in *Winged Shield, Winged Sword: A History of the United States Air Force* Vol. I, ed. Bernard C. Nalty, (Washington D.C., United States Air Force,1997), 390.

[48] Wolk, "From Air Service to Air Corps: The Era of Billy Mitchell," in *Winged Shield, Winged Sword: A History of the United States Air Force* Vol. I, ed. Bernard C. Nalty, (Washington D.C., United States Air Force,1997), 396

[49] GEN Keith Alexander, House Armed Services Subcommittee, Cyberspace Operations Testimony, Washington D.C., September 23, 2010.

[50] GEN Keith Alexander, "Building a New Command in Cyberspace", *Strategic Studies Quarterly*, (Summer, 2011): 9.

[51] GEN Keith Alexander, House Armed Services Subcommittee, Cyber Operations Testimony, March 27 2012.

[52] US Government Accounting Office *Defense Department Cyber Efforts, More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities* (Washington, DC: US Government Accountability Office, May 2011), 11.

[53] US Government Accounting Office *Defense Department Cyber Efforts, More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities*, 12.

[54] US Department of Defense, *Quadrennial Roles and Missions Review Report* (Washington, DC: U.S. Government Printing Office, July 2009), 16.

[55] Elisabeth Bumiller, "Pentagon Expanding Cybersecurity Force to Protect Networks Against Attacks," *New York Times,* January 27, 2013.

[56] GEN Keith Alexander, House Armed Services Subcommittee, Cyberspace Operations Testimony, Washington D.C., September 23, 2010.

[57] GEN Keith Alexander, House Armed Services Subcommittee, Cyberspace Operations Testimony, Washington D.C., September 23, 2010.

[58] US Government Accounting Office *Defense Department Cyber Efforts, More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities,* 18.

[59] US Government Accounting Office *Defense Department Cyber Efforts, More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities,* 19.

[60] Holger Stark, "Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War," *Der Speigel Online*, (August 8, 2011), http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html (accessed March 13, 2013).

[61] Col Phillip S. Meilinger, "Giulio Douhet and the Origins of Airpower Theory," in *The Paths of Heaven,* ed. Col Phillip S. Meilinger (Maxwell AFB, Ala.: Air University Press, 1997), 2.

[62] Hearings before the President's Aircraft Board, September 1925 (Washington, D.C.: Government Printing Office, 1925), 599.

[63] J.R. Wilson, MARFORCYBER: "Marines Fight in a New Domain", *Defense Online* (February 4, 2013), http://www.defensemedianetwork.com/stories/marforcyber-marines-fight-in-a-new-domain/ (accessed March 13, 2013).

[64] GEN Keith Alexander, House Armed Services Subcommittee, Cyberspace Operations Testimony, Washington DC, September 23, 2010..

[65] COL Greg Conti and COL John "Buck" Sudru, email message to author, February 19, 2013.

[66] Captain Frank A. Shaul, *Command and Control of the Department of Defense in Cyberspace*, Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, April 2011); COL Jeffery A. May, *A Model for Command and Control of Cyberspace, Strategy Research Project* (Carlisle Barracks, PA: U.S. Army War College, April 2011)

[67] USCODE Title 10-Armed Forces (2011), Enclosure 5, Section 2.c.(1).

[68] US Navy Seals Home Page, http://www.sealswcc.com/navy-seals-overview.aspx#.UUEBoqXF--Q, (accessed March 13, 2013). US Army Rangers Home Page, http://www.army.mil/ranger/, (accessed March 13, 2013). US Air Force Special Ops Home Page, http://www.airforce.com/specialops. (accessed March 13, 2013).

[69] J.R. Wilson, MARFORCYBER: "Marines Fight in a New Domain", *Defense Online* (February 4, 2013), http://www.defensemedianetwork.com/stories/marforcyber-marines-fight-in-a-new-domain/ (accessed March 13, 2013).

[70] Giulio Douhet, The Command of the Air, trans. Dino Ferrari (1942; reprint, Washington, D.C.: Office of Air Force History, 1983), 30.

[71] John Baumgartner, "Smart Grid Vulnerabilities to Cyber Attacks" in *The Energy and Security Nexus: A Strategic Delemma*", ed. Carolyn W. Pumphrey, (Carlisle Barracks, PA, Strategic Studies Institute, USAWC, November 2012), 230.

[72] William Mitchell, *Skyways: A Book on Modern Aeronautics* (Philadelphia, PA: J. B. Lippincott Co., 1930), 5.