REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
09-05-2017	Master's Thesis	SEP 2016 - MAY 2016

4. TITLE AND SUBTITLE

A Work in Progress: The Human Dimension in Cyberspace

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Glisson, Holly, A., Major, US Army

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

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

USMC Command and Staff College
Marine Corps University
2076 South Street

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Department of Defense should establish a separate cyber service in order to man and train the best possible force to fight in cyberspace. The US military component services have made significant progress in recruiting and training their cyber forces, but there is room for improvement. Now is the time to institute major changes to the cyber force. A dedicated cyber service would be small, grown from USCYBERCOM, and would bear little resemblance to any other military service, but would retain Title 10 authorities. Creating a separate, premier cyber force will ensure the United States' ability to

15. SUBJECT TERMS

Cyberspace; Force Structure; Cyber personnel

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
Unclass	Unclass	Unclass	UU	33	19b. TELEPHONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:

A Work in Progress: The Human Dimension in Cyberspace

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:

Glisson, Holly A., United States Army

AY 16-17

Mentor and Oral Defense Committee Member: _____
Approved: _____
Date: _____

Oral Defense Committee Member: _____
Approved: _____
Date: _____

Executive Summary

Title: A Work in Progress: The Human Dimension in Cyberspace

Author: Glisson, Holly A., United States Army

Thesis: The Department of Defense should establish a separate cyber service in order to man and train the best possible force to fight in cyberspace.

Discussion: Seven years after the inception of USCYBERCOM, it is time to analyze the necessity for a separate cyber service within the Department of Defense. The US military component services have made significant progress in recruiting and training their cyber forces, but there is room for improvement. The services are still working to build training programs and fill cyber billets. Now is the time to institute major changes to the cyber force – while the culture is still malleable.

Conclusion: Identified recommendations to improve the military's cyber forces can be executed by establishing a separate cyber service. This cyber service would be small, grown from USCYBERCOM, and would bear little resemblance to any other military service, but would retain Title 10 authorities. Creating a separate, premier cyber force will ensure the United States' ability to dominate in all domains of war.

DISCLAIMER (Printing Section II)

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

List of Illustrations

Page

List of Tables

No table of figures used.

Table of Contents

Preface

I arrived at US Army Human Resources Command in May 2014. Serving as an assignment officer in US Army Signal Branch, I worked in the same room as the officers building the US Army's first ever Cyber Branch. With backgrounds in signal, electronic warfare, and combat arms, the officers and non-commissioned officers working in the cyber assignment branch reflected the desired skills of future Army cyber officers. They worked closely with Army cyber units, carefully crafting Military Personnel (MILPER) messages to the force, providing instructions on how to become a cyber officer and what they were looking for. As Army leaders described what an ideal cyber officer looks like – strategy minded, combat arms experience, holds a computer science related degree, dabbles in network design as a hobby – Cyber branch joked that the ideal cyber candidate was akin to a mythical unicorn. They quickly adopted the unicorn as their unofficial mascot. For Halloween, they even dressed up as unicorn hunters with weapons fashioned out of keyboards.

As the Army was birthing its cyber force, it was simultaneously executing a drawdown. Responding to massive budget cuts, the Army was forced to downsize over 20% of its personnel. The Army's first Officer Separation Board (OSB) results were released in the summer of 2014. The boards targeted those with low performance or derogatory files, but the system was not perfect, and the Army lost officers with valuable skill sets. For example, a telecommunication systems engineering officer, earning his PhD in the same field, was selected for separation. One of many, this type of loss crippled the growth of the cyber force. Also due to the drawdown, the Army could not afford to recruit additional members to build its cyber branch, they could only transfer existing officers from other career fields.

The first wave of officers accepted for branch transfer into the newly minted cyber branch were predominantly officers already serving in cyber command billets. The cyber training pipeline was not yet established, so the transfer board selected officers with on the job experience. I fielded several calls from frustrated signal officers not selected for the transfer. Officers with STEM degrees and civilian cyber certifications were left wondering how the Army was going to determine if they were a good fit for cyber from an officer record brief. I was left wondering if the Army chose the best officers to stand up cyber branch – or if they just chose people who happened to serve in the right place at the right time.

During the same timeframe, the Army was heavily scrutinized for its methods of talent management. In 2015, Lieutenant General (Retired) David Barno published a widely read article in *The Atlantic*, titled, "Can the US Military Halt its Brain Drain?" He criticized the Army's lack of talent management and rigid career timelines as the cause of talented officers voluntarily leaving the active duty service. To address the issue, the Army stood up a Talent Management Task Force, led by a two-star general. The task force is still addressing and testing methods of talent management. This past year, Army HRC launched Assignment Interactive Module 2.0, a pilot program intended to identify talents and match officers with better suited assignments.

In this climate of cyber growth, fiscal constraint, and talent management concerns, I question whether we are building the best possible cyber force, and how it can be done. Not only are we hunting unicorns, we are trying to fit round pegs into square holes. Why not make the holes round? People do not have to fit the mold of a Soldier, Airmen, Sailor, or Marine to be a great cyber warrior. Selecting cyber warriors only from this specific population may preclude us from recruiting the very best cyber talent. By definition, what is not the best, is second rate. The

United States invests massive resources to maintain a constant state of readiness to engage in warfare. Our military should not be in the business of being second rate.

Introduction

"Victory smiles upon those who anticipate the change in the character of war, not upon those who wait to adapt themselves after the changes occur." –Giulio Douhet[1]

The United States has reigned as the world's most powerful military since World War II, continuously maintaining an asymmetric advantage in technology, equipment, and training. From strategic air power, to nuclear weapons, to a range of technology produced by the Second and Third Offset Strategies, the United States sustained military superiority by changing the character of war at every turn.[2] For the first time, the US military may find itself behind the curve in the virtual arms race of cyberspace, adapting instead of leading the change. At a Cyber Symposium in February 2017, the Air Force Chief Information Officer, Lieutenant General William Bender likened US cyber capabilities to being behind in the Super Bowl, requesting a lot of brain power to pull off a come-from-behind victory.[3] Whether US cyber capabilities are truly behind is debatable, but the cyber domain is widely regarded as a level playing field, overturning the familiar mindset that the United States is accustomed to unparalleled technological resources.[4]

Vulnerability in cyberspace offers a means for adversaries to overcome US advantages in conventional military power – in ways that are instantaneous, difficult to trace the source of,[5] and nearly impossible to anticipate. Cyber operations are inherently covert. How can the strength of an adversary's cyber capability be measured? The International Institute for Strategic Studies in London publishes an assessment of global military powers annually, tallying and comparing the personnel and equipment of over 170 countries.[6] When it comes to cyber forces, however, even the institute recognizes that capabilities cannot be assessed quantitatively.[7] Offensive cyber

capabilities require less equipment and are easier to hide than the proliferation of aircraft carriers or nuclear weapons – making it easy to publicly downplay cyber assets. Cyberwarfare is merely a battle of wits between humans. Therefore, the most important factor in determining the strength of a military's cyber program is the skill of the people behind it. The human dimension is the most critical element in ensuring success in cyberspace.

On the surface, it seems logical to create a cyber force separate from the other military services. Each of the other domains have a dedicated service. Why not cyber? More importantly, a separate cyber force would enable DoD leadership to define the prerequisites of a cyber warrior outside the constraints required of a Soldier, Airman, Sailor, or Marine. Creating a separate cyber force to increase the pool of potential cyber personnel, improve training, and address organizational challenges, is not an original idea. The notion has been written about at every level in every branch of the military. Retired Navy Admiral James Stavridis proposed a separate cyber force in *Proceedings Magazine* in 2014. He likened the cyber force to the creation of the US Air Force, suggesting the military bypass the 20 year debate surrounding the elevation of the US Army Air Corps to a separate service.[8] Army Colonel Charles C. Rimbey considered a separate cyber service in his strategy research project at the US Army War College.[9] Navy Captain Don Donegan proposed using the Navy-Marine Corps relationship as a blueprint, creating a US Cyber Corps as a separate service within the Department of the Air Force.[10] These officers identified several shortfalls that have since been addressed since the inception of US Cyber Command (CYBERCOM). The US military has made great strides in rapidly building cyber forces and developing training programs – but it may never be enough. The most optimal construct for waging cyber operations is to create a separate cyber service. This service should still be part of the military for ease of joint planning and Title 10 purposes, but should bear little

resemblance to the rest of the military. This standalone service would be composed of a different breed of fighters, with innate cyber talent and carefully fostered cyber expertise, ensuring the United States continues its military asymmetric advantage into the cyber domain.

To emphasize the necessity of a separate cyber service, this paper will discuss and further develop previously made arguments, and analyze the effects of recent efforts by the DoD to improve cyber capabilities by:

1) Discussing the complexity of what cyberspace means.

2) Reviewing the development of CYBERCOM.

3) Discussing challenges related to recruiting and retaining cyber personnel.

4) Discussing challenges related to training cyber personnel.

5) Assessing the progress made to address the manning and training challenges.

6) Discussing organizational concerns and provide recommendations.

Seven years have passed since the activation of CYBERCOM, the organization responsible for implementing the above goals. It is still a work in progress, but it is time to evaluate said progress and determine if the arguments for a separate cyber force are still valid.

CYBERCOM

Secretary of Defense Robert Gates considered several options leading up to the establishment of CYBERCOM in 2010. The director of national intelligence at the time, Mike McConnell, urged him to create a separate combatant command to deal with cyber threats as early as 2008. Because the Department of Defense was in the midst of establishing another new

combatant command, AFRICOM, Secretary Gates opted to establish CYBERCOM as a subordinate unit of STRATCOM.[11] It made sense for the NSA director to lead CYBERCOM, as they had the resources and were effectively in charge of the cyber mission already.[12] Secretary Gates also admitted this decision was partly motivated to promote the NSA director, Keith Alexander, to a four-star General.[13] The plan was always to elevate CYBERCOM to full combatant command status.[14] By 2015, Secretary of Defense Ash Carter took this a step further and speculated the possibility of a separate cyber service. When asked about the possibility of creating a separate cyber service, he responded, "I think you have to look at this as the first step in a journey that may, over time, lead to the decision to break out cyber the way that you said the Army Air Corps became the U.S. Air Force… we have given some thought to that. And for right now, we're walking before we run. But… that's one of the futures that cyber might have."[15] His comments underscore the uncertainty of CYBERCOM's future. Former and current CYBERCOM leadership do not support the establishment of a separate cyber service. Retired General Keith Alexander believes CYBERCOM should operate as a unified-functional command, like US Special Operations Command (SOCOM).[16] The current CYBERCOM Commander, Admiral Michael Rogers, agrees.[17] This goal is short sighted. CYBERCOM is not analogous to SOCOM. Special Operations is not a domain. The military is the preponderant source for the best SOF candidates, whereas the best reservoir for preexisting cyber skills is in the civilian workforce.[18] To man and train the best force to fight in the cyber domain, CYBERCOM needs to become a separate service.

What is Cyberspace?

"Mr. President, the problem is much worse than you think." –General John Vessey

Cyber is an adjective primarily used as a prefix. Merriam-Webster simply defines the meaning of cyber as "of, relating to, or involving computers or computer networks."[19] Cyber is now a buzzword, and slang usage is quickly making it an ill-defined noun. The conversation surrounding cyberwarfare elicits several questions on the nature of cyberspace as a domain. Is cyber war coming?[20] Is cyberspace even a warfighting domain?[21] If cyberspace is not a domain, should it be treated like a geographic command? How does cyberwar relate to cybersecurity and who should be responsible for each? What delineates a cybercrime from a cyber act of war? The ambiguity of cyberwar makes it difficult to determine whether CYBERCOM's current formation adequately meets the needs of potential war via cyberspace.

The first presidential directive on cybersecurity predates the first computer worm, unleashed in 1988. After viewing the 1983 film, *WarGames*, President Reagan asked his Joint Chiefs of Staff to investigate the possibility and potential damage of an attack via computer telecommunications.[22] The Chairman at the time, General John Vessey, quickly discovered the reality and magnitude of the threat. The following year, President Reagan signed National Security Decision Directive Number 145 (NSDD-145), elevating what is now known as cybersecurity to a national political level. Over the next three decades, the world became exponentially reliant on computer systems, and the cyber issue continued to grow in importance.

Although contested by some, Cyberspace is now widely regarded as the fifth domain of war. In July of 2016, NATO recognized cyberspace as a domain of operations in which the alliance must defend itself as effectively as it does in the air, on land, and at sea.[23] Cyberspace

operations can crosscut every physical warfighting domain - no modern military can perform in battle without reliance on cyberspace.[24] Satellites, guided munitions, nuclear launch systems, unmanned aerial vehicles, and countless other communication dependent technologies require connectivity through the cyber domain.[25] In 2011, the DoD's global cyberspace architecture included over 15,000 networks and seven million computing devices – the largest in the world.[26] It is still growing. While the United States reaped enormous benefits from this capability, it also became increasingly vulnerable in cyberspace. To address this growing threat, cyber warfare efforts were continuously elevated and cyberspace became a domain to protect.

Aside from simply describing cyber operations as offense or defense, there are two main efforts when discussing military actions in cyberspace. The first effort is a combination of active defense and deterrence. Actions in cyberspace are covert and often undetected. Furthermore, the only difference between a cyber act of war and a cybercrime is the purported intent behind the action. Bob Stasio, the former Chief of Operations at NSA's Cyber Center prior to the creation of CYBERCOM, described the center as being in "constant crisis mode." Military networks were constantly being probed and scanned by hackers looking for vulnerabilities.[27] The fight in cyberspace is constant, whether the US is involved in a conflict or not. Cyber harassment is now a common tool used in the gray zone – the space between peace and war.[28] In cyberspace, the line between gray zone cyber activity and cyber acts of war is blurred. Acts of war are tied to the second effort in cyberspace: operations enabling kinetic strikes in the other domains. An example of an action in this effort is Stuxnet, which constituted a computer network attack, causing physical damage across international boundaries, destroying a fifth of Iran's nuclear centrifuges.[29] Another example is Israel's ability to bomb Syria undetected by disabling radar

detection of an incoming strike. Israel accomplished this feat in 2007.[30] Both of these cyberspace efforts call attention to capabilities that are the responsibility of CYBERCOM.

The Emergence of US Cyber Command

"Our current cyber quandary is not some passing phase – it is the new normal for the joint force." - US Cyber Command Action Group[31]

In October of 2008, a NSA analyst discovered a breach on a classified, air gapped military network in US Central Command.[32] The NSA quickly developed a plan, code-named Buckshot Yankee, to counter the malware. The source of the cyberattack was never confirmed publicly, so the intent of the attack is unknown, but Buckshot Yankee catalyzed the establishment of US Cyber Command. Defense Secretary Robert Gates announced the creation of CYBERCOM in 2009. Prior to its creation, the signal community primarily defended the network and the intelligence community primarily conducted offense. As Keith Alexander later told a congressional committee in 2010, "It became clear that we needed to bring together the offense and defense capabilities."[33] To provide a fledgling CYBERCOM with resources, CYBERCOM is co-located with the NSA, sharing a dual-hatted commander. This union further blurs the line between jurisdictions in cyberspace, as CYBERCOM operates under Title 10 authority as a military entity, and the NSA operates under Title 50 authority, covering intelligence activities and covert action.[34]

While the NSA focuses on cryptology, Signals Intelligence, Information Assurance, and enabling Computer Network Operations (CNO),[35] CYBERCOM's mission statement is:

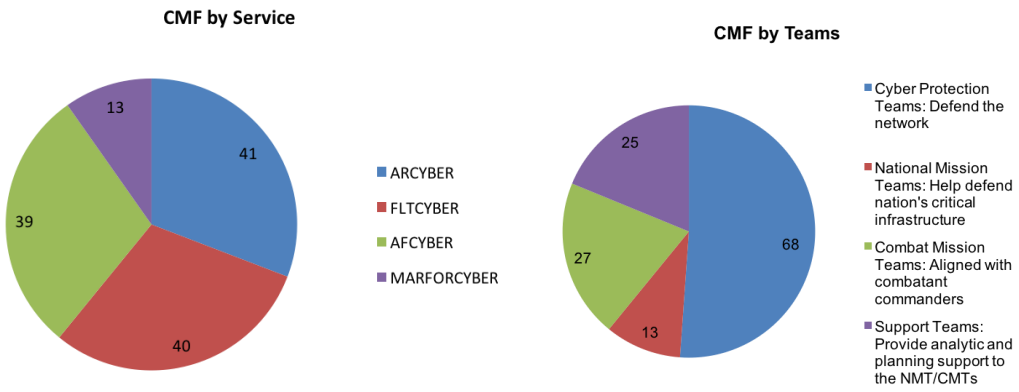
> USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.[36]

The command has three main focus areas. The first two areas of focus are to direct the operations and defense of specified Department of Defense information networks (DODIN), and to conduct full spectrum military cyberspace operations in order to enable actions in all domain. These two areas of focus imply a support role of CYBERCOM to the existing services. However, the third focus area, to ensure US/Allied freedom of action in cyberspace and to deny the same to adversaries, is outside the scope of the other domains – and outside the scope of the existing service branches.[37] CYBERCOM's mission resembles that of a service level organization. The latter portion is parallel to the US Navy's mission to maintain freedom of the seas.[38]

Prior to the creation of CYBERCOM, the Air Force initiated development of a unit focused solely on cyberspace in 2006. The initial intent was to add cyberspace to its existing domains of air and space, making the Air Force the lead service to own the cyberspace mission. It is still included in their mission statement: "The mission of the United States Air Force is to fly, fight and win in air, space and cyberspace."[39] Facing leadership challenges over the course of the next two years, the Air Force delayed the creation of Air Force Cyber Command, finally demoting the conceptual unit to a numbered command under Air Force Space Command, culminating in the activation of the 24th Air Force (24AF) in 2009. With the advent of CYBERCOM, the Air Force began to build distinct cyber career fields in 2010.[40] The number of cyber airmen quadrupled between 2010 and 2016, aligned with the rapid expansion of the CYBERCOM mission.[41]

In conjunction with the activation of CYBERCOM, the Army, Navy, and Marines also established component commands within a year. In order to rapidly fill its ranks, each branch filled cyber positions with existing service members, primarily from the signal, intelligence, and electronic warfare fields. Later, a requirement surfaced for an agile force ready to engage

adversaries in a tactical cyber fight on order. This requirement spurred the development of the Cyber Mission Force (CMF). Initiated in 2013, the CMF includes National Mission Teams, Combat Mission Teams, and Cyber Protection Teams. The DoD's goal is to have 133 teams by 2018.[42] Each service is responsible for providing the personnel to fill these teams, dividing the responsibility like slices of pie:



In 2015, the DoD outlined five strategic goals in its Cyber Strategy:

1. Build and maintain ready forces and capabilities to conduct cyberspace operations;

2. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions;

3. Be prepared to defend the U.S homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence;

4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages;

5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.[43]

The strategy went on to emphasize the priority of building the Cyber Mission Force first, identifying three foundational pillars: enhanced training; improved military and civilian recruitment and retention; and stronger private sector support.[44] CYBERCOM is close to reaching its goal of becoming fully functional by 2018. In October 2016, the CMF reached initial operating capability. Comprised of 5,000 individuals across 133 teams, the CMF needs to grow to 6,200 to become fully operational.[45] This doesn't include anticipated personnel growth as the cyber mission expands. CYBERCOM is moving in the right direction, but developing capability in cyberspace is more than recruiting a certain quantity of people. The rapid development and dynamic nature of the cyber domain requires people with agile cyber skills and expert training.

Recruiting and Retaining Challenges

"The cyber trenches must include pure geeks, with an unparalleled command of coding, and emotionally intelligent social scientists." – Retired Admiral James G. Stavridis[46]

As the United States becomes more reliant on technology, demand for cybersecurity specialists is outpacing supply. The United States is experiencing a "human capital crisis" in its cybersecurity workforce, as described by the Center for Strategic and International Studies.[47] An estimated 30,000 unfilled cybersecurity jobs exist in the US federal government alone.[48] The demand for cyber skilled personnel will only continue to grow. How can CYBERCOM recruit top notch cyber personnel in such a strained field?

Be all that you can be. Accelerate your life. We do the impossible every day. The few, the proud, the Marines. The US military excels at recruiting kinetic warfighters, as seen in these slogans by the Army, Navy, Air Force, and Marine Corps. But the US Armed Forces are not currently well suited to recruit, develop, and retain the talent required to successfully operate in

the cyber domain.[49] The Army recently launched an ad campaign specifically to recruit cyber personnel. A commercial, released in late 2016, begins with a voiceover of a fictional hacker describing cyberattacks, and ends with the message, "For every would-be cyberattack, there's a team of U.S. Army Cyber Warriors who will not be defeated."[50] The commercial is a step in the right direction, but the military must overcome the public's undesirable perceptions of working in the Army and promise a more unique and impactful occupation than a cybersecurity job in the private sector.

The ideal cyber warrior must have a high technical aptitude and be a creative problem solver. The ideal cyber warrior must also have a hacker mindset – one who enjoys manipulating complex systems and pushing technology in ways unintended by its designers.[51] The profile of a hacker evokes dated images of a social recluse - a nerd in a dark room bearing no resemblance to military warrior. This image is not an accurate description of what a hacker looks like, then or now. James Lance, a cybersecurity expert and head of cyber intelligence at Deloitte and Touche, describes the qualities of a good hacker: risk-taking, extreme self-confidence, the compulsion to break things to understand them, and the desire for recognition.[52] He went on to explain, "Hackers need validation."[53] While there is some overlap, the qualities listed above do not quite fit the military mold, where discipline and uniformity are paramount and physical brawn is a cherished attribute - and for good reason. But different qualities are now needed of cyber warriors, and what this ideal should look like is still being debated within military ranks.

For the potential cyber warriors that may fit the military culture, there are countless civilian job opportunities that are more financially lucrative with better talent management and career progression options. These factors may inhibit the existing military services from recruiting the best cyber talent as CYBERCOM grows. The overwhelming majority of the

current cyber force was selected from the existing military population – which accounts for less than 1% of the entire US population. Imagine the talent the cyber force could recruit if the pool of potential personnel increased beyond 1% of the population. That need to access a greater pool of talent weighs heavily on US military leaders.

It is important to note that "cyber skilled personnel" is an all-encompassing term. Cyber skills can vary from specialization in coding, to engineering infrastructure, to hacking. Of this broad range of skills, hacking, in particular, is a difficult skill to identify and recruit. Hacking used to have negative connotation, as it was once only defined as illegal or unauthorized activity. Hacking is now more broadly regarded as the use of technical expertise to overcome a problem in cyberspace, such as exploiting or identifying vulnerabilities in a network.[54] In 2010, Army LTC Gregory Conti, then Director of West Point's Cyber Security Research Center, conducted a survey on Slashdot.org to gain a sense of the technical community's perception of the military. Some perceptions were positive, but the majority of responses indicated perceptions of low pay, poor career advancement opportunities, limited creativity, lifestyle inflexibility, bias against non-combat personnel, technology ignorant leadership, and misutilization.[55]

Since 2010, sweeping policy changes, such as the repeal of Don't Ask Don't Tell and the integration of women into combat arms, have slightly altered some of the perceptions of military cultue, but the characteristics behind most the of the perceptions above still remain. If anything, the reputation of the DoD was degraded in recent years by high profile media stories such as the Edward Snowden NSA leaks and the Marines United scandal. In July 2012, General Alexander, then Commander of USCYBERCOM and NSA, gave a speech at DefCon, one of the world's largest hacking conferences held annually in Las Vegas. Instead of his uniform or a suit, he wore jeans and a black shirt as he called on the attendees to come work for him.[56] He shed his uniform

in an attempt to be more appealing to the hackers, acknowledging and avoiding characteristics of the military that do not coincide with the cyber community's. A year later, his invite to speak at DefCon was rescinded in the wake of the Edward Snowden incident. Instead, he appeared at another hacking convention called Black Hat, where he was heckled by the audience.[57] The hacker community, filled with talented cyber workers, does not have a positive opinion of the DoD.

The military image is at a nadir. On the one hand, the existing branches of the military are strict, bureaucratic, and uncompromising in standards. On the other hand, recent exposes such as high profile sexual assault cases and indiscriminate killing, indicate the military is toxic. Either way, the current image of the military contributes to a divide between the military and civilians. Until US cyber forces can divorce themselves from this image and the perceptions identified in the survey above, it will be difficult to find, court, and hire the best cyber talent.

To build the cyber force rapidly, the services recruited personnel already serving on active duty. As the cyber force expands and accepts new members, the DoD can select cyber recruits from the entire US population – but only those who meet the existing initial entry requirements of each service. Lifting the physical requirements would drastically increase the pool of candidates, enabling the military to choose from a wider range of talent. Cyber warriors do not need to meet height and weight requirements or be physically fit to do their job. Tattoos, physical disabilities, and age have no bearing on whether a person is a genius at coding or finding vulnerabilities in an adversary's network. For example, removing certain physical requirements would no longer preclude an individual with flat feet from serving in the cyber force – as it would preclude the same individual from joining the Army.

In the cyber domain, technical prowess is revered over physical aptitude.[58] Commitment and loyalty standards should remain, but physical traits are less important. To address this notion, the United Kingdom allows relaxed grooming standards for cyber warriors.[59] However, current US military leadership are not willing to compromise these standards. When asked about the possibility of relaxed physical or appearance standards for cyber warriors, the Marine Corps Commandant did not budge - General Neller replied, "They will be Marines."[60] This sentiment is understandable, because the Marine Corps views all members as Marines first, a priority over their occupational specialty. This demand is unnecessary for the cyber force, most cyber operations are conducted remotely from the battlefield. The priority should be focused on cyber personnel being the world's best in cyber operations.

An undergraduate student at Purdue University recently conducted a survey to determine average salaries at top tech companies. His survey of recent graduates with a bachelor's degree revealed salaries the DoD cannot compete with.[61] The salaries of recent top college graduates are comparable to an O-5 in the military, with almost 20 years of service.[62] For the military to acquire these top tech graduates, cyber recruiters have to compete with the salary disparity by finding ways to offer attractive incentives. The nobility and romance of serving your country only goes so far. To overcome this, the military is looking at initial entry at higher ranks, and targeting high school aged cyber talent for college scholarship programs.

Once recruited into the military, cyber personnel require different career timelines. The skill set and personality of this skilled workforce is inherently different than the rest of the military. Members of the existing service branches adhere to strict career timelines, with promotions bound more to time in service than merit or skill. There is no jumping the ladder or remaining on a rung. In his criticism of talent management, retired LTG Barno pointed out issues

of "up or out" promotion.[63] Military personnel are not permitted to stay in the same rank or job year after year – even if the position may be one they are perfectly suited to fill. Not only must military personnel constantly compete for promotion, they are forced out if not selected for advancement.[64] This is especially problematic for the cyber force. If a person's specialized skills make them perfectly suited for a certain position, why force them to either move or separate? The military has overcome issues like this before. Each service can create exceptions to policy to assist in recruitment and retention. The Army's medical branch, for example, allows for lateral entry for medical professionals and their promotion schedule is separate from the rest of the Army's branches. While exceptions to policy are feasible, it would be more fruitful to design career management specifically tailored to the cyber forces – something that could be accomplished by a standalone cyber force.

Training Challenges

"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." – GEN Alexander, during a Congressional testimony, when asked how CYBERCOM will improve the department's ability to provide a trained cyber force.[65]

Each branch of the military has come a long way in developing their cyber training programs since the advent of CYBERCOM in 2010. Prior to the existence of CYBERCOM, none of the military services had a career field specializing in cyberspace operations. The only training in this arena were auxiliary certification courses for signal or intelligence personnel. Now, each branch of service has a cyber training pipeline for both enlisted personnel and commissioned officers.

The US Naval Academy received $120 million in federal funding to build a Center for Cyber Security Studies. The cyber center will include 206,000 square feet of secure training facilities.[66] The US Army runs a separate Army Cyber Institute at West Point and a Cyber Center of Excellence at Fort Gordon, Georgia. The US Air Force runs a Cyber College under Air University at Maxwell Air Force Base, Alabama and cyber classes at the Air Force Institute of Technology at Wright-Patterson Air Force Base in Ohio. Contrary to GEN Alexander's vision, USCYBERCOM personnel are trained separately by their service branches, as opposed to one, streamlined, standardized training pipeline. Cyber personnel from each branch of the military report to USCYBERCOM influenced by their service's legacy doctrine, thus introducing an element of confusion within the joint cyber ranks.[67] Divergent thinking is not necessarily a bad thing, but personnel working at the strategic level may find themselves at odds with mission accomplishment if what is best for CYBERCOM is not aligned with what is best for their service. Aside from this concern, the individual services are spending a great deal of money building separate cyber training institutions. Building one cyber institution for the entire military would save funds and consolidate the best training resources and instructors. This one institution could include initial cyber enlisted training, a cyber service academy, professional military education courses, enlisted training – everything cyber housed in one collaborative location.

To compound recruiting issues, the military is struggling to train the quantity of cyber personnel required for the joint Cyber Mission Force in addition to service specific cyber billets. Exacerbating this issue is the nature of the cyber mission. The constant nature of the cyber mission means cyber personnel are constantly engaged in the fight, leaving little time for training. The Operational Test and Evaluation (DOT&E) Office of the Secretary of Defense identified several issues with training the cyber force in its 2016 annual report on Cybersecurity.

It described a reinforcing loop straining the operators serving on cyber Red Teams. Over the past seven years, Red Team operators have become high demand assets. Many of these cyber experts left the DoD to accept positions in the private sector, citing higher wages and a more relaxed work environment.[68] This led to a personnel shortage that increased the operational tempo of the remaining Red Team operators, reducing training opportunities "to the extent they are not able to keep pace with the tool and skill sets of advanced cyber adversaries."[69] The high operational tempo contributes to the attrition of Red Team operators. The attrition of red team operators then contributes to an even higher operational tempo, which leads to less time for training - reinforcing the loop.

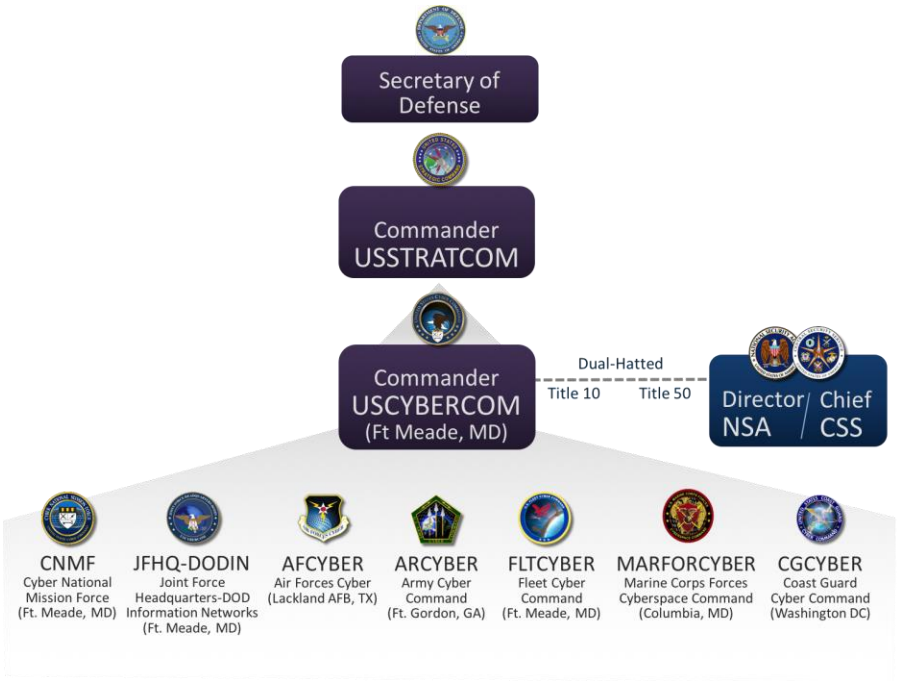
In its assessment of Cyber Protection Teams, DOT&E reported that the current Cyber Protection Team (CPT) elements "have not received the adequate training or equipment required to provide effective and timely support to defend networks and critical missions."[70] The initial staffing of the CPTs, pulled from the existing services, included personnel without requisite skills and training. Military personnel entered the cyber force at all levels of leadership with little related experience. To mitigate the lack of proficiency, CYBERCOM invests in expensive training regimens, paying millions of dollars to transform soldiers, sailors, airmen, and marines to cyber fighters. Instead of combining efforts towards one top quality institution, USCYBERCOM is discovering how to conduct joint training events while the individual services frantically – and redundantly - build their training centers.

Organizational Concerns

"Cyberspace operations demand unprecedented degrees of collaboration, which the US government must approach holistically." - US Cyber Command Combined Action Group[71]

In cyberspace, efficiency and speed of communication are critical to mission success. Cyber effects can traverse the globe in about .17 seconds – about the time it takes to blink.[72] The speed and viral nature of cyberattacks can inflict collateral damage not bound by country borders.[73] Centralized command and control is imperative. Apart from command and control, however, geography is irrelevant. Cyber fighters can operate from anywhere and affect any domain.

That nature of CYBERCOM's composition can potentially undermine unity of effort. A cohesive branch would best serve national security objectives, but the elements making up CYBERCOM will maintain institutional allegiance to their services. As long as cyber personnel belong to the Army, Air Force, Navy, or Marines, they will at least be partially influenced by another domain.[74] Each service's cyber force is supporting two missions – that of their service and that of the joint CYBERCOM force. The current task organization of USCYBERCOM includes all the services' cyber commands, the Cyber National Mission Force, and the Joint Headquarters for DoD Information Networks. These subordinate elements, in addition to that of the NSA, indicate a large span of control for the CYBERCOM Commander:



The culture of each existing service focuses on their assigned domain. The Army prioritizes land. The Navy prioritizes the sea. The Air Force prioritizes the air. The Marines prioritize expeditionary maneuver in the physical domains. Who is prioritizing cyber? Most warfighting elements are culturally reticent to think of cyber personnel as warriors affecting front line operations, cognitively separating cyber from weapons used to fight wars.[75] The teams making up the Cyber National Mission Force are assigned responsibility by geographic area, not by physical domains. The teams need working knowledge of how the other services operate, but allegiance to a service is not necessary.

Progress: The Current State of US Cyber Command

"The greatest challenge faced by the DoD – and the entire government – is human resources. Technological dominance is meaningless without a skilled workforce capable of operating at the highest level of their field. In this area, we are falling short." –Representative Jim Langevin[76]

Progress in cyber innovation since 2010 is incredible. The DoD quickly delivered manning and budget documents, enabling the services to rapidly build their cyber warfare capabilities. There are now over 5,000 employees assigned to the CMF, with a budget roughly over half a billion dollars. The DoD's overall cyber budget for fiscal year 2017 is $6.7 billion. Services are taking great strides to meet the demands of the CMF and the warfighting units of their individual services. Each branch of the military is in the process of building their cyber branches, focusing first on creating training programs.

In 2013, the United States Naval Academy was the first service academy to offer Cyber Operations as a major. Members of the Naval Academy Class of 2016 were the first to graduate with a Cyber Operations degree. The Army quickly followed. In 2014, they officially created a cyber branch within the Army, creating new cyber centric military occupational specialties (MOS) for both officers and enlisted personnel. The United States Military Academy at West Point runs the Army Cyber Institute (ACI) and directly commissions 2LTs into cyber branch. The ACI also runs a Cyber Leader Development Program (CLDP).[77] Beyond the building of cyber institutions, the services are also working together to provide top tier training through inter-service and international hackathons.

In an effort to overcome cyber manning challenges, the US Air Force built programs in an effort to lure cyber talent into their ranks. For example, a program called "Stripes for Certification" provides opportunities to enlist at higher grades when entering the Air Force with cyber-related certifications. Similar to the Army, the Air Force instituted a Cyberspace Warfare Operations career track for officers, to provide proper growth opportunities.[78] The Air Force is also targeting potential cyber warriors before they reach college. The Air Force Association's "Cyber Patriot" initiative, in which Airmen mentor youth cyber teams, involves over 20,000

students across the nation.[79] This initiative is a great example of how cyber should use atypical recruitment methods to identify young cyber talent. Advertising cyber as its own service, with its own appealing identity, would aid and foster atypical recruitment methods.

To compete with lucrative jobs in the civilian sector, Congress is considering incentives to recruit cyber warriors. One such example is the previously discussed opportunity for lateral entry. The military currently allows lateral entry for medical professionals. Most doctors enter service as an O-3. Similarly, an experienced cyber professional recruited from a top civilian institution should be able to enter service at a military grade that reflects their skills and experience.

The DoD drastically improved internal cyber training, are willing to adjust policies to recruit the best cyber talent, and are working to improve inter-service collaboration through the CMF, but are these efforts enough to ensure we will have the best possible cyber force? Despite these efforts, there is room for improvement.

The Air Force's new occupational specialty, Cyber Warfare Operations, is currently only manned at 46 percent, principally due to rapidly increasing requirements.[80] The Army's cyber occupational specialties are also undermanned. The attempt to fill the cyber positions affected related military occupational specialties as well. US Army signal functional area officers and warrant officers are filled at less than 50% as those officers were moved to fill cyber positions.

In December of 2016, President Obama signed the National Defense Authorization Act[81], which authorized the elevation of CYBERCOM to a full combatant command. In his remarks, President Obama went on to express support for ending the dual hat arrangement for the NSA and CYBERCOM, but "maintaining shared capabilities and synergies developed under the dual

hat arrangement."[82] This is a step towards the original intent for CYBERCOM, but cyber is not equivalent to a geographic region. It is a domain that transcends geography.

The key difference between the mission of a geographic combatant command, as opposed to a service commands, is that the services focus on manning, training, and equipping, while the geographic combatant commands control operations in their assigned areas. Separating cyber as its own service will allow for a unified effort in manning, training, and equipping the cyber force. The cyber force would still have representation on joint staffs, just as any other service, to ensure they are properly integrated in strategic operations.

Recommendations

"Cyber cannot be a buzzword that is used to obtain larger portions of the budget or secure contracts. Cyber must be a term that belongs to a specific community that is truly operational. Cyber must be its own community and have its own leaders. Those who say cyber personnel are too technical to lead their own are only trying to find a way to stay relevant in a domain they do not understand." -1st Lt. Robert M. Lee, USAF, while serving as a cyber team leader in 2013.[83]

To improve recruiting, retention, training, and command relationships, there are several steps the DoD can make:

1) Create a cyber test similar to the ASVAB. An entry test for transfers will help identify skills not currently depicted in personnel files. The test would also indicate which field in cyber will be best suited for the candidate.

2) Adjust physical standards. Cyber personnel do not require physical fitness standards, height and weight standards, or grooming and appearance standards to complete their missions. Physical disabilities should also be waived.

3) Traditional boot camps and basic training courses are not necessary for cyber personnel.

4) Increase the frequency of Training with Industry (TWI) opportunities, or allow cyber personnel to separate and reenter the force after gaining experience in the private sector.

5) Create one cyber education institution for all services. This would save DoD funds by consolidating resources. Creating one institution would facilitate one streamlined, standardized training program.

The best way to institute these recommendations is to create a separate cyber service, focused on building high quality cyber experts. This service would be unlike any other military organization, changing the image of what military service looks like. The cyber service may not resemble what the world views as military, but would operate under Title 10 code. It would be small, and organized similarly to CYBERCOM, but would take on the role of manning, training, and equipping its own forces. As the Army, Navy, and Marines maintained a small footprint of aircraft when the Air Force was created, the other services would still maintain a small footprint of cyber personnel at the Division level - but strategic cyber missions would be the purview of the standalone cyber service. The signal and communications personnel of each service would continue to defend their tactical level networks.

Conclusion

The ultimate enabler of the cyber force is the people behind it. In times of fiscal austerity, the military is often charged to do more with less. The military services prioritized the creation of its cyber forces, but executed the build-up in a way that made economic sense. Instead of actively pursuing the best cyber talent across the United States, the military predominately selected existing members and then turned them into cyber warfighters. Whether those fighters were made into cyber experts remains to be seen.

The Army, Navy, Air Force, and Marines invested significant resources to build US CYBERCOM. Early on, military leadership identified potential shortfalls in manning and training cyber personnel and made several efforts to overcome those shortfalls. While CYBERCOM is nearing full functionality, other measures can be taken to improve the quality of US cyber forces. A separate cyber service does not have to look like the other services – it just needs the people it requires to perform the requisite Title 10 functions. Above all, the United States requires a cyber service to ensure it has the world's foremost cyber force to continue to dominate every domain of war.[84] Separating the cyber force will improve the cyber culture and remove limitations of the current services, opening the door a little wider to go out and recruit the best cyber talent. The nation's adversaries are becoming stronger in cyberspace every day. If CYBERCOM is indeed behind in developing cyber capabilities, it cannot close the gap with a second rate cyber force.

Notes

[1] Richard H. Estes, "Guilio Douhet: More on Target Than He Knew," *Airpower Journal*, Winter 1990, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj90/win90/6win90.htm.
[2] Timothy A. Walton, "Securing the Third Offset Strategy: Priorities for the Next Secretary of Defense," *Joint Force Quarterly 82,* July 2016: 6. http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-82/Article/793224/securing-the-third-offset-strategy-priorities-for-the-next-secretary-of-defense/.
[3] Tom Roeder, "Air Force's Top Computer Warfare Expert Says US Has Fallen Behind," *Colorado Springs Gazette,* February 2, 2017, http://gazette.com/air-forces-top-computer-warfare-expert-says-u.s.-has-fallen-behind/article/1596250.
[4] Damien Paletta, Danny Yadron, and Jennifer Valentino-Devries, "Cyberwar Ignites a New Arms Race," *The Wall Street Journal*, October 11, 2015, accessed March 1, 2017. https://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128.
[5] William J. Lynn, "Defending a New Domain," *Foreign Affairs* (Sep/Oct 2010): 108.
[6] International Institute for Strategic Studies, *The Military Balance 2017*, London, UK, 2017, http://www.iiss.org/en/publications/military%20balance/issues/the-military-balance-2017-b47b.
[7] Paletta, *The Wall Street Journal,* October 11, 2015.
[8] James Stavridis, "Time for a US Cyber Force," *Proceedings Magazine,* January 2014, https://www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force.
[9] Charles C. Rimbey, "Off We Go Into the Wild Digital Yonder: Building Cyber Forces," Master's thesis, US Army War College, 2013, http://www.dtic.mil/docs/citations/ADA590666.
[10] Don Donegan, "Towards a National Cyber Force 'Department of the Air Force – US Cyber Corps,'" *Center for International Maritime Security,* December 21, 2015, http://cimsec.org/20754-2/20754.
[11] Robert M. Gates, *Memoirs of a Secretary at War* (New York: Random House LLC, 2014), 449.
[12] Shane Harris, *@War: The Rise of the Military Internet Complex* (New York: Houghton Mifflin Harcourt Publishing, 2014), 48.
[13] Gates, 440.
[14] Harris, 48.
[15] Ash Carter, "Remarks to US Cyber Command Work Force," Speech, Fort Meade, MD, March 13, 2015, accessed February 1, 2017, https://www.defense.gov/News/Transcripts/Transcript-View/Article/607024/remarks-by-secretary-carter-to-us-cyber-command-workforce-at-fort-meade-maryland/.
[16] Joe Gould, "Former NSA Chief: Follow SOCOM Model for CYBER," *Defense News,* April 17, 2015, http://www.defensenews.com/story/defense-news/blog/intercepts/2015/04/17/keith-alexander-cyber-dod-aei/25951903/.
[17] Mark Pomerleau, "Rogers: Cyber Doesn't Need its Own Military Branch," *Defense Systems*, January 21, 2016, https://defensesystems.com/articles/2016/01/21/rogers-cyber-doesnt-need-to-be-separate-branch.aspx.
[18] Christopher Paul. "The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces." *Rand Corporation* 2014, 41. http://www.rand.org/pubs/research_reports/RR780.html.
[19] *Merriam-Webster Online*, s.v. "cyber," accessed March 1, 2017, https://www.merriam-webster.com/dictionary/cyber.

[20] Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013).
[21] Martin C. Libicki, "Cyberspace is Not a Warfighting Domain," *Rand Corporation*, January 1, 2012, http://www.rand.org/pubs/external_publications/EP51077.html.
[22] Fred Kaplan, *Dark Territory* (New York: Simon and Schuster, 2016), 1.
[23] "Cyber Defence." *North Atlantic Treaty Organization*, February 17, 2017, http://www.nato.int/cps/en/natohq/topics_78170.htm.
[24] Francesca Spidalieri and Jennifer McArdle, "Transforming the Next Generation of Military Leaders: The Role of Cybersecurity Education in the US Service Academies," *Cyber Defense Review*, 2010: 141. http://www.cyberdefensereview.org/.
[25] *Ibid*, 141.
[26] *Ibid*, 144.
[27] Harris, 82.
[28] Michael J. Mazarr, "Mastering the Gray Zone: Understanding a Changing Era of Conflict," *Small Wars Journal*, December 2015: 59, http://smallwarsjournal.com/blog/mastering-the-gray-zone-understanding-a-changing-era-of-conflict.
[29] Jon R. Lindsey, "Stuxnet and the Limits of Cyber Warfare." *Security Studies*, Volume 22, August 1, 2013, http://www.tandfonline.com/doi/abs/10.1080/09636412.2013.816122.
[30] David A. Fulghum, "Israel Used Electronic Attack in Air Strike Against Syrian Mystery Target," *ABC News*, October 8, 2007, http://abcnews.go.com/Technology/story?id=3702807&page=1.
[31] US Cyber Command Action Group, "Beyond the Build: How Component Commands Support the US Cyber Command Vision," *Joint Forces Quarterly* 80, 1st Quarter 2016: 93. http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_86-93_CyberCom.pdf.
[32] Harris, 149.
[33] *Ibid*, 150.
[34] Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence, Activities & Covert Action," *Harvard National Security Journal, Vol. 3.*, Harvard Law School, 2011. http://harvardnsj.org/2011/12/demystifying-the-title-10-title-50-debate-distinguishing-military-operations-intelligence-activities-covert-action/.
[35] "Mission and Strategy," *NSA*.gov, last modified August 19, 2016, https://www.nsa.gov/about/mission-strategy/.
[36] "US Cyber Command Factsheet," *US Strategic Command*, September 30, 2016, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/.
[37] *Ibid.*
[38] "Mission," *Navy.com*, accessed 1 March 2017, https://www.navy.com/about/mission.
[39] "Mission," *AirForce.com*, accessed 1 March 2017, https://www.airforce.com/mission.
[40] William E. Parker, "Cyber Workforce Retention," *Air University Press* (October 2016): 9.
[41] *Ibid*, 10.
[42] "The Department of Defense Cyber Strategy," *US Department of Defense*, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/.
[43] US Department of Defense, *The DoD Cyber Strategy*, Washington, DC, April 2015, 13, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.
[44] *Ibid*.

[45] US Cyber Command News Release, "All Cyber Mission Force Teams Achieve Initial Operating Capability," *US Department of Defense News*, October 24, 2016, https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/.
[46] James Stavridis, "Time for a US Cyber Force," *Proceedings Magazine*, January 2014, https://www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force.
[47] William Parker, "Cyber Workforce Retention," *Perspective on Cyber Power, Air Force Research Institute*, Air University Press, Maxwell Air Force Base, AB, October 16, 2016, 2, http://www.au.af.mil/au/aupress/bookinfo.asp?bid=600.
[48] *Ibid*.
[49] Gregory Conti and Jen Easterly, "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture," *Small Wars Journal* (July 29, 2010), smallwarsjournal.com/printpdf/9443.
[50] "US Army Commercial: Cyber," YouTube Video, October 24, 2016, 0:31, https://www.youtube.com/watch?v=0LZnOorfS_Q.
[51] Gregory Conti and Jen Easterly, "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture," *Small Wars Journal* (July 29, 2010), smallwarsjournal.com/printpdf/9443.
[52] Jon Schuppe, "Born at the Right Time: How Kid Hackers Became Cyberwarriors." *NBC News*, Dec 30, 2014, http://www.nbcnews.com/news/us-news/born-right-time-how-kid-hackers-became-cyberwarriors-n273916.
[53] *Ibid.*
[54] *Wikipedia*, s.v. "Hacker," accessed April 29, 2017, https://en.wikipedia.org/wiki/Hacker.
[55] Gregory Conti and Jen Easterly, "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture," *Small Wars Journal* (July 29, 2010): 2, smallwarsjournal.com/printpdf/94432.
[56] Harris, 67.
[57] *Ibid*, 68.
[58] Gregory Conti and Jen Easterly, "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture," *Small Wars Journal* (July 29, 2010): 2, smallwarsjournal.com/printpdf/94432.
[59] Ben Farmer, "New Army Cyber Warriors Allowed Long Hair," *The Telegraph*, March 26, 2016, http://www.telegraph.co.uk/news/2016/03/26/new-army-cyber-warriors-allowed-long-hair/.
[60] Hope Seck, "Service Chiefs Reject Proposal to Develop New Military Cyber Force." *Military.com*, February 22, 2016. http://www.military.com/daily-news/2016/02/22/service-chiefs-reject-proposal-develop-new-military-cyber-force.html.
[61] Lora Kolodny, "What interns and new grads really get paid at top tech companies," https://techcrunch.com/2016/12/02/what-interns-and-new-grads-really-get-paid-at-top-tech-companies/.
[62] DFAS, "Military Pay Charts," https://www.dfas.mil/militarymembers/payentitlements/military-pay-charts.html.
[63] David Barno and Nora Bensahel, "Can the U.S. Military Halt Its Brain Drain?" *The Atlantic* (November 5, 2015), https://www.theatlantic.com/politics/archive/2015/11/us-military-tries-halt-brain-drain/413965.
[64] *Ibid*.

[65] Charles C. Rimbey, "Off We Go Into the Wild Digital Yonder: Building Cyber Forces," Master's thesis, US Army War College, 2013, 14, http://www.dtic.mil/docs/citations/ADA590666.
[66] Francesca Spidalieri and Jennifer McArdle, "Transforming the Next Generation of Military Leaders: The Role of Cybersecurity Education in the US Service Academies," *Cyber Defense Review*, 2010, 157, http://www.cyberdefensereview.org/.
[67] James Stavridis, "Time for a US Cyber Force," *Proceedings Magazine*, January 2014, https://www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force.
[68] Director, Operational Test and Evaluation. "Cybersecurity." *FY 2016 Annual Report*, http://www.dote.osd.mil/pub/reports/FY2016/.
[69] *Ibid.*
[70] *Ibid.*
[71] US Cyber Command Combined Action Group. "Beyond the Build: How the Component Commands Support the U.S. Cyber Command Vision." *Joint Forces Quarterly* 80, 1st Quarter 2016: 86. http://www.dtic.mil/doctrine/jfq/jfq-80.pdf.
[72] David C. Hathaway, "The Digital Kasserine Pass: The Battle Over Command and Control of DOD's Cyber Forces." *Foreign Policy at Brookings*, July 15, 2011, 5, handle.dtic.mil/100.2/ADA561493.
[73] *Ibid*.
[74] Stavridis, *Proceedings Magazine*, January 2014.
[75] Jacquelyn Schneider and Nina Kollars, "Cyber Beyond the Third Offset: A Call for Warfighter-led Innovation." *War on the Rocks*, January 5, 2017, https://warontherocks.com/2017/01/cyber-beyond-third-offset-a-call-for-warfighter-led innovation.
[76] Francesca Spidalieri and Jennifer McArdle, "Transforming the Next Generation of Military Leaders: The Role of Cybersecurity Education in the US Service Academies," *Cyber Defense Review*, 2010, 142, http://www.cyberdefensereview.org/.
[77] "Cyber Leader Development Program Overview," *United States Military Academy*, http://www.usma.edu/acc/SitePages/CLDP.aspx.
[78] Pomerleau, Mark. "DOD's Long Path to Creating a Cyber Warrior Workforce." *Defense Systems*, March 4, 2016, https://defensesystems.com/articles/2016/03/04/dod-cyber-warrior-workforce.aspx.
[79] *Ibid*.
[80] William Parker. "Cyber Workforce Retention." *Perspective on Cyber Power, Air Force Research Institute.* Air University Press, Maxwell Air Force Base, AB, October 16, 2016, xiii, http://www.au.af.mil/au/aupress/bookinfo.asp?bid=600.
[81] "National Defense Authorization Act for Fiscal Year 2017." H.R. 4909, 114th Congress, https://www.congress.gov/bill/114th-congress/house-bill/4909/text.
[82] "Statement by the President on Signing the National Defense Authorization Act for Fiscal Year 2017." *Office of the Press Secretary, The White House*, December 23, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/12/23/statement-president-signing-national-defense-authorization-act-fiscal.
[83] Robert M. Lee, "The Failing of Air Force Cyber," *Signal Magazine – AFCEA International*, November 1, 2013, http://www.afcea.org/content/?q=failing-air-force-cyber.

[84] Charles C. Rimbey, "Off We Go Into the Wild Digital Yonder: Building Cyber Forces," Master's thesis, US Army War College, 2013, 21, http://www.dtic.mil/docs/citations/ADA590666.

Bibliography

Alexander, Keith. “Speech on US Cybersecurity Policy and the Role of US CYBERCOM.” Washington, DC. June 3, 2010. https://www.nsa.gov/news-features/speeches-testimonies/speeches/100603-alenander-transcript.shtml

Arnold, Todd, Rob Harrison, and Gregory Conti. “Towards a Career Path in Cyberspace Operations for Army Officers.” *Small Wars Journal,* August 18, 2014. http://smallwarsjournal.com/jrnl/art/towards-a-career-path-in-cyberspace-operations-for-army-officers

Barno, David and Nora Bensahel. “Can the U.S. Military Halt Its Brain Drain?” *The Atlantic,* November 5, 2015. https://www.theatlantic.com/politics/archive/2015/11/us-military-tries-halt-brain-drain/413965/

Brantly, Aaron F. “Cyber Actions by State Actors: Motivation and Utility.” *International Journal of Intelligence and Counterintelligence,* May 12, 2014. http://www.tandfonline.com/doi/abs/10.1080/08850607.2014.900291

Broder, Jonathon. “Alex Gubney’s Disturbing New Film Explains Why Cyberwar is Here to Stay.” *Newsweek Tech & Science*, July 7, 2016. http://www.newsweek.com/2016/07/22/zero-days-stuxnet-cyber-warfare-478565.html

Carter, Ash. “Remarks by Secretary Carter to US Cyber Command Workforce at Fort Meade, Maryland.” Speech. Fort Meade, MD, March 13, 2015, US DoD News Transcript. http://archive.defense.gov/transcripts/transcript.aspx?TranscriptID=5602

Center for Strategic and International Studies. “Significant Cyber Incidents Since 2006.” CSIS Headquarters, 2017. https://www.csis.org/programs/technology-policy-program/cybersecurity/significant-cyber-incidents

Chen, Thomas. “An Assessment of the Department of Defense Strategy for Operating in Cyberspace.” *The Letort Papers, Strategic Studies Institute,* September, 2013. http://www.globalsecurity.org/security/library/report/2013/ssi_chen.pdf

Clark, Richard A. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: HarperCollins, 2010.

Conti, Gregory and David Raymond. “Leadership of Cyber Warriors: Enduring Principles and New Directions.” *Small Wars Journal*, July 11, 2011. http://smallwarsjournal.com/jrnl/art/leadership-of-cyber-warriors-enduring-principles-and-new-directions

Conti, Gregory, John Nelson, and David Raymond. “Towards a Cyber Common Operating Picture.” *5th International Conference on Cyber Conflict*, NATO CCD COE Publications, 2013. https://ccdcoe.org/cycon/2013/proceedings/d1r2s4_conti.pdf

Conti, Gregory and Jen Easterly. “Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture.” *Small Wars Journal*, July 29, 2010. smallwarsjournal.com/printpdf/9443.

Director, Operational Test and Evaluation. “Cybersecurity.” *FY 2016 Annual Report*. http://www.dote.osd.mil/pub/reports/FY2016/

Duggan, Patrick. “Harnessing Cyber-Technology’s Human Potential.” *Special Warfare, Volume 28, Issue 4,* October-December 2015. http://www.soc.mil/swcs/SWmag/archive/SW2804/October%202015%20Special%20Warfare.pdf

Farmer, Ben. “New Army Cyber Warriors Allowed Long Hair.” *The Telegraph*, March 26, 2016. http://www.telegraph.co.uk/news/2016/03/26/new-army-cyber-warriors-allowed-long-hair/

Flynn, Matthew J. “Is there a Cyber War?” *National Cybersecurity Institute Journal,* Volume 1, *No. 2*, Excelsior College, 2014. http://www.excelsior.edu/static/journals/nci-journal/1-2/offline/download.pdf

Harris, Shane. *@War: The Rise of the Military Internet Complex.* New York: Houghton Mifflin Harcourt Publishing, 2014.

Hathaway, David C. “The Digital Kasserine Pass: The Battle Over Command and Control of DOD’s Cyber Forces.” *Foreign Policy at Brookings*, July 15, 2011. handle.dtic.mil/100.2/ADA561493

International Institute for Strategic Studies. *The Military Balance 2017*, London, UK, 2017. http://www.iiss.org/en/publications/military%20balance/issues/the-military-balance-2017-b47b

Kane, Tim. *Bleeding Talent.* New York: Palgrave Macmillan, 2012.

Kaplan, Fred. *Dark Territory: The Secret History of Cyber War*. New York: Simon and Schuster, 2016.

Lee, Robert M. “The Failing of Air Force Cyber.” *Signal Magazine - AFCEA International*, November 1, 2013. http://www.afcea.org/content/?q=failing-air-force-cyber

Libicki, Martin C. “Cyberspace Is Not a Warfighting Domain.” *Rand Corporation*, January 1, 2012. http://www.rand.org/pubs/external_publications/EP51077.html

Lindsay, Jon R. “Stuxnet and the Limits of Cyber Warfare.” *Security Studies, Volume 22*, August 1, 2013. http://www.tandfonline.com/doi/abs/10.1080/09636412.2013.816122

Lyle, Amaani. “Motivation, Talent Remain Strongest Elements of Network Defense, Says Cyber Official.” *DoD News, Defense Media Activity*, October 25, 2016. https://www.defense.gov/News/Article/Article/985385/motivation-talent-remain-strongest-elements-of-network-defense-says-cyber-office

Lynn III, William J. “Defending a New Domain.” *Foreign Affairs, Vol. 89, Issue 5*, September/October 2010. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

Mullins, Barry. “Developing Cyber Warriors from Computer Engineers.” *American Society for Engineering Education*, 2012. https://www.asee.org/public/conferences/8/papers/3146/download

Paletta, Damian, Danny Yadron, Jennifer Valentino-Devries. “Cyberwar Ignites a New Arms Race.” *The Wall Street Journal*, October 11, 2015. https://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128

Parker, William E. “Cyber Workforce Retention.” *Perspective on Cyber Power, Air Force Research Institute Papers*, Air University Press, Maxwell Air Force Base, Alabama, October 16, 2016. http://www.au.af.mil/au/aupress/bookinfo.asp?bid=600

Paul, Christopher, Isaac R. Porche III, and Elliot Axelband. “The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces.” *Rand Corporation* 2014. http://www.rand.org/pubs/research_reports/RR780.html

Pomerleau, Mark. “DOD’s Long Path to Creating a Cyber Warrior Workforce.” *Defense Systems*, March 4, 2016. https://defensesystems.com/articles/2016/03/04/dod-cyber-warrior-workforce.aspx

Pellerin, Cheryl. “Rogers Discusses Near Future of US Cyber Command.” *DoD News, Defense Media Activity*, February 24, 2017. https://www.defense.gov/News/Article/Article/1094167/rogers-discusses-near-future-of-us-cyber-command/

Ramsby, Corey. “A Reality Check on a Cyber Force.” *Strategic Studies Quarterly*, Summer 2016. http://www.dtic.mil/dtic/tr/fulltext/u2/1015715.pdf

Rector, Kenneth A. “Message from the Commandant.” *US Army Cyber School Quarterly Newsletter*, February 2017. https://cyberschool.army.mil

Rid, Thomas. *Cyber War Will Not Take Place*. New York: Oxford University Press, 2013.

Rimbey, Charles. “Off We Go Into the Wild Digital Yonder: Building Cyber Forces.” Master’s thesis, Unites States Army War College, 2013. www.dtic.mil/docs/citations/ADA590666

Rustici, Ross M. “Cyberweapons: Leveling the International Playing Field.” *Parameters, Vol. 41, Issue 32,* September 2011. http://connection.ebscohost.com/c/articles/73781214/cyberweapons-leveling-international-playing-field

Schneider, Jacquelyn, and Nina Kollars. “Cyber Beyond the Third Offset: A Call for Warfighter-led Innovation.” *War on the Rocks,* January 5, 2017. https://warontherocks.com/2017/01/cyber-beyond-third-offset-a-call-for-warfighter-led innovation/

Schuppe, Jon. “Born at the Right Time: How Kid Hackers Became Cyberwarriors.” *NBC News,* Dec 30, 2014. http://www.nbcnews.com/news/us-news/born-right-time-how-kid-hackers-became-cyberwarriors-n273916

Shakarian, Paulo. “Stuxnet: Cyberwar Revolution in Military Affairs.” *Small Wars Journal,* April 15, 2011. http://smallwarsjournal.com/jrnl/art/stuxnet-cyberwar-revolution-in-military-affairs

Shinkman, Paul D. “America is Losing the Cyber War.” *US News and World Report,* September 29, 2016. https://www.usnews.com/news/articles/2016-09-29/cyber-wars-how-the-us-stacks-up-against-its-digital-adversaries

Spidalieri, Francesca and Jennifer Mcardle. “Transforming the Next Generation of Military Leadership into Cyber Strategic Leaders: The Role of Cybersecurity in US Service Academies.” *Cyber Defense Review,* Spring 2010. http://www.cyberdefensereview.org/

Stavridis, James, and David Weinstein. “Time for a U.S. Cyber Force.” *Proceedings Magazine Vol 140/1/1,331 (2014).* https://www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force

Stone, John. “Cyber War Will Take Place!” *Journal of Strategic Studies, Volume 36, 2013,* November 29, 2012. http://www.tandfonline.com/doi/abs/10.1080/01402390.2012.730485?journalCode=fjss20

Tilghman, Andrew. “In Supersecret Cyberwar Game, Civilian Sector Techies Pummel Active-duty Cyberwarriors.” *Military Times,* August 4, 2014. http://www.militarytimes.com/story/military/tech/2014/08/04/in-supersecret-cyberwar-game-civilian-sector-techies-pummel-active-duty-cyberwarriors/13566549/

Thompson, Nicholas. “The Former Secretary of Defense Outlines the Future of Warfare.” *Wired,* February 19, 2017. https://www.wired.com/2017/02/former-secretary-defense-outlines-future-warfare/

US Congress. House. *National Defense Authorization Act for Fiscal Year 2017*. HR 4909. 114th Cong., Calendar No. 502 (May 26, 2016). https://www.congress.gov/bill/114th-congress/house-bill/4909/

US Cyber Command Combined Action Group. “Beyond the Build: How the Component Commands Support the U.S. Cyber Command Vision.” *Joint Forces Quarterly 80, 1st Quarter 2016*, http://www.dtic.mil/doctrine/jfq/jfq-80.pdf

US Department of Defense. *The DoD Cyber Strategy*. Washington, DC, April, 2015. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Wall, Andru E. “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence, Activities & Covert Action.” *Harvard National Security Journal, Vol. 3.*, Harvard Law School, 2011. http://harvardnsj.org/2011/12/demystifying-the-title-10-title-50-debate-distinguishing-military-operations-intelligence-activities-covert-action/

Walton, Timothy A.“Securing the Third Offset Strategy: Priorities for the Next Secretary of Defense,” *Joint Force Quarterly 82*, July 2016. http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-82/Article/793224/securing-the-third-offset-strategy-priorities-for-the-next-secretary-of-defense/

Yannakogeorgos, Panayotis A. and John P. Geis II. “The Human Side of Cyber Conflict: Organizing, Training, and Equipping the Air Force Cyber Workforce.” *Air University Press*, June 2016. http://www.au.af.mil/au/aupress/bookinfo.asp?bid=595