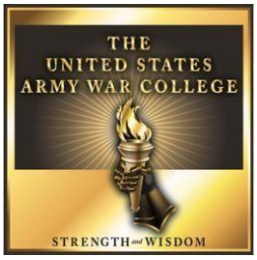
Strategy Research Project

Recruiting, Developing, and Retaining a Competent and Capable Cyber Workforce

by

Mr. Darrell D. McCarthy
Department of the Army

Under the Direction of:
Colonel John Sena



United States Army War College
Class of 2017

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-04-2017	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Recruiting, Developing, and Retaining a Competent and Capable Cyber Workforce

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Mr. Darrell D. McCarthy
Department of the Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel John Sena

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.

To the best of my knowledge this SRP accurately depicts USG and/or DoD policy & contains no classified information or aggregation of information that poses an operations security risk. **Author:** ☒ **PA:** ☒

13. SUPPLEMENTARY NOTES
Word Count: 6041

14. ABSTRACT

Cybersecurity is one of the United States' most strategic vulnerabilities. Rogue nations, state and non-state actors are using cyber as a strategic weapon against the United States and its allies. To effectively counter this risk, the United States and its allies need to develop a robust cybersecurity posture. This essentially means having the most advanced technology to counter, coerce, and deter aggressive and nefarious cyber activities coupled with an appropriate response should the need arise. Advanced technology also requires highly trained cyber professionals to operate within the cyber space domain. Since the Department of Defense is the organization that has the mission to defend the homeland from cyber-attacks and mitigate the effects thereof, this SRP analyzes the current Department of Defense cyber recruitment efforts, its training and development strategy, whether the strategy supports the requirement to build technically competent capacity quickly, and how to retain the talent necessary to dominate the cyber domain. I also provide recommendations on how the Department of Defense can achieve their strategic goals.

15. SUBJECT TERMS
Recruitment, Development, and Retention

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** *(w/ area code)*
UU	UU	UU	UU	27	

Recruiting, Developing, and Retaining a Competent and Capable Cyber Workforce

(6041 words)

Abstract

Cybersecurity is one of the United States' most strategic vulnerabilities. Rogue nations, state and non-state actors are using cyber as a strategic weapon against the United States and its allies. To effectively counter this risk, the United States and its allies need to develop a robust cybersecurity posture. This essentially means having the most advanced technology to counter, coerce, and deter aggressive and nefarious cyber activities coupled with an appropriate response should the need arise. Advanced technology also requires highly trained cyber professionals to operate within the cyber space domain. Since the Department of Defense is the organization that has the mission to defend the homeland from cyber-attacks and mitigate the effects thereof, this SRP analyzes the current Department of Defense cyber recruitment efforts, its training and development strategy, whether the strategy supports the requirement to build technically competent capacity quickly, and how to retain the talent necessary to dominate the cyber domain. I also provide recommendations on how the Department of Defense can achieve their strategic goals.

Recruiting, Developing, and Retaining a Competent and Capable Cyber Workforce

> Many of our adversaries lack the ability to confront our forces physically, choosing instead to employ virtual weapons with potentially devastating effect. We must take full advantage of these technologies, building our own capabilities to operate in cyber-space with the same level of skill and confidence we enjoy on the land. We will either adapt to this reality or risk ceding the advantage to future enemies.
>
> —General Raymond T. Odierno[1]

The United States (U.S.), its allies, and partners face an extremely fluid strategic environment that continues to challenge leaders in establishing and executing policies and strategies that will secure the United States national interests. As the Operational Environment and Army Learning Training Circular outlines, the strategic environment remains as it has always been—complex. The current strategic environment seems more ambiguous, presenting multiple layers of complexity and a multiplicity of actors challenging the Army with requirements beyond traditional warfighting skills and training. A wide-range of actors across current and projected environments–friendly and neutrals, malicious actors, and threats–will interact often in an uncoordinated manner to produce a complex environment. Neutral or even friendly actors act in accordance with organizational goals that may be contrary to U.S. national interests and cause friction. Malicious actors use violence in pursuit of their goals and will potentially challenge U.S. national interests and vulnerabilities. Threats will use this complexity to their advantage and often employ hybrid strategies. This multiplicity of actors will continue to operate across operational environments during the foreseeable future.[2] Therefore, it is in the interests of the United States to pursue innovative ideas with the purpose of protecting the homeland and defending against conventional and nonconventional attacks.

The enduring national interests of the United States are clearly delineated in the most recent version of the National Security Strategy. Of those that are considered the typical challenges to the strategic environment (i.e., failed states, terrorism, counter weapons of mass destruction), cyberspace has truly emerged to be one of the most significant strategic risks to the United States and its allies. Since 1969, the tool that was initially used to share data between scientists, the internet, has become a global force that changed the way the world operates.[3] This new tool has grown exponentially to connect almost every person around the world. Money Magazine by Time, quoted a report from the International Telecommunications Union that estimated that in 2015, over 3 billion people used the internet. The number of internet users has increased from 738 million in 2000 to 3.2 billion in 2015. That's a seven-fold increase that brought internet penetration up from 7% to 43% of the global population.[4] With this number of people using the internet, there are bound to be some who use it to create conflict and potentially war.

For decades, terms like landpower, air power, sea power, and similar prefixes for domains have been used and one can somewhat deduce how those are defined just by the words “land,” “air,” and “sea.” However, with the creation of the internet, and although most were not aware of the revolutionary change it would bring, a new potential domain has emerged. Businesses, academia, government, and most institutions in the United States and in other developed and even developing countries, rely heavily on the use of the internet. Its use has made an indelible mark on how we communicate today and in the future vice how we communicated in the late 1960s and early 1970s.

From the 1960s through today, technology has become more advanced and increasingly complex that it is challenging to maintain a competitive advantage in cyber. Some of the earliest attacks on computer networks highlighted the vulnerability of the internet and the massive amount of damage it can do to a network if appropriate cybersecurity controls and protocols are not enacted. Some of those early attacks are underscored in an article by the Daily Beast. In that article, the Daily Beast highlights the top 10 most infamous hacking attacks in the U.S. I will discuss three of these events and as time progressed each will show the reader how sophisticated each attack was compared to the previous attack.

In 1988, Robert Tappan Morris, while enrolled as a graduate student at Cornell University, designed a self-replicating worm and gave it a mission: go out to determine the size of the internet.[5] It backfired, replicating itself beyond control as it infected thousands of computers (a lot at the time!), cost millions of dollars in damage, and inspired the U.S. government to create an emergency response for computers—Computer Emergency Response Team.[6] Morris was eventually charged under the Computer Fraud and Abuse Act for his accidental crimes and ordered to pay $10,000 and do 400 hours of community service.[7] The source code was archived on a black 3.5-inch floppy disk now on display at the Boston Museum of Science.[8]

In 1999, New Jersey-resident David L. Smith gave a stripper in Florida a computer virus that bared her name.[9] Using a stolen *America Online* (AOL) account, Smith posted a Word document infected with "Melissa" to a discussion group on AOL, purporting it to be a list of usable log-in information to pornography sites.[10] Smith's virus spread via email, forwarding itself to fifty email accounts in Microsoft Outlook on every

infected computer, and which, over time, overloaded email servers and forced companies such as Microsoft, Intel, Lockheed Martin, and Lucent Technologies to shut down their email networks.[11] In the end, “Melissa” infected one million personal computers and caused $80 million dollars in damage.[12]

Considered one of the worst hackings in the United States was in 2014 when the Office of Personnel Management (OPM) was compromised twice and the personal information of over 21 million people was stolen. The OPM is the federal government’s human resources department, and has the task of conducting background checks for security clearances. Marina Koren, a senior associate writer with The Atlantic, stated that the breach, attributed to China, occurred in December 2014 and was made public in early June 2015.[13] The Obama administration estimated that security clearance data—including fingerprints, Social Security numbers, addresses, employment history, and financial records—of 4 million people was exposed. In July 2015, the administration revised that estimate to 21.5 million after a second intrusion was detected.[14]

With the examples provided, cyberspace is a domain that will be extremely difficult to control. It continually poses a strategic security threat to the U.S. and its allies and will require innovative offensive and defensive solutions to counter rogue nations and actors from inflicting irreparable damage to the United States. Cybersecurity has become one of the nation’s top priorities and strategic risks that if not managed and resourced, could be nefariously used to degrade our ability to detect and respond to hostile cyber-attacks. At the heart of the issue is the requirement to build the necessary capacity and capability to deter the threat and mitigate the impacts of a cyber-attack. Naturally, this means people with the requisite knowledge, skills, abilities, and

competencies will be obligatory. The focus of this paper will be to analyze the current Department of Defense (DOD) cyber recruitment efforts, its training and development strategy, whether it supports the requirement to build technically competent capacity quickly, and how to retain the talent necessary to dominate the cyber domain.

Background

Cybersecurity has become one of the nation's top priorities and strategic risks that if not managed and resourced, could be nefariously used to degrade our ability to detect and respond to hostile cyber-attacks. The 2015 *National Security Strategy* states, "To maintain our military edge and readiness, we will continue to insist on reforms and necessary investment in our military forces and their families."[15] Our military will remain ready to deter and defeat threats to the homeland, including against missile, cyber, and terrorist attacks, while mitigating the effects of potential attacks and natural disasters.[16] The DOD is the federal agency tasked with the role of defending the United States homeland and its interests including cyber-attacks.[17] The *DOD Cyber Strategy* discusses the United States' role in the creation of the internet and the urgent need for international laws that govern its responsible use.[18] As the U.S. has lead the international order and in the land, air, and sea domains, the U.S. will be expected to lead the world in developing the technology to deter adversaries who wish to use cyber in a nefarious manner, but also be able to respond to cybersecurity attacks. Therefore, on June 23, 2009, the Secretary of Defense directed the Commander, U.S. Strategic Command establish a sub-unified command, United States Cyber Command (USCYBERCOM).[19] The USCYBERCOM mission is to plan, coordinate, integrate, synchronize and conduct activities to: direct the operations and defense of specified DOD information networks and; prepare to, and when directed, conduct full spectrum

military cyberspace operations to enable actions in all domains, ensure United States' and Allies' freedom of action in cyberspace and deny the same to our adversaries.[20] Therefore, the United States has engaged with other nations, including academia and business, to ensure we develop innovative solutions to deter and deny access to our critical infrastructure and sensitive networks. The DOD strategy outlines the need to build a capable cyber workforce with the requisite knowledge, skills, and abilities to successfully defend against cyber-attacks and protect valuable DOD information infrastructure.[21]

The Department's strategy outlines five strategic goals. The primary strategic goal that will be discussed in this paper is the goal of building and maintaining cyber ready forces and capabilities to conduct cyberspace operations that will enable the DOD in defending the DOD information network, secure DOD data, and mitigate risks to DOD missions.[22] Build and maintain cyber forces and capabilities to conduct cyberspace operations is a strategic goal that if successful will be the first and last line of defense for all that is done in cyberspace.[23] DOD must have the right people at the right time to protect and defend against attacks in cyberspace. If DOD cannot recruit, train, and retain the right people with the requisite skills, then DOD will not fulfill its mission to defend the homeland against cyberspace attacks. A precision-like focus on the recruitment, training and development, and retention of the cyber workforce from an enterprise level perspective is required. They will require a shift in the culture to ensure this type change is communicated and institutionalized. While each personnel category will have its ways and means to execute the strategy, a comprehensive strategic approach is best. Recruitment is an important factor in achieving the strategic goal, but

having the capacity without the appropriate capability (training) and platforms to prevent talent drain (retention) does little for the DOD. Hence, it is important that the department has the requisite recruitment, development, and retention strategies that will facilitate achievement of the goal.

Recruitment Strategy

The Cyber Mission Force is composed of three sets of forces aligned to achieve USCYBERCOM's three primary missions.[24] Those sets are the Cyber National Mission Force, Cyber Combat Mission Force, and Cyber Protection Force. Once fully manned, trained, and equipped in FY 2018, these 133 teams comprising the Cyber Mission Force will execute the three primary missions with approximately 6,200 military and civilian personnel.[25]

As previously discussed, the DOD has a strategic goal to build and maintain a capable and formable cyber workforce.[26] As Major General Stephen Fogarty, Former Commanding General, Army Cyber Command stated,

> The dynamic nature of the cyberspace operational environment, and increasingly high operational risk posed by cyberspace actors requires the Army to act now. The Army must adapt and change the way we develop concepts and capabilities, and educate and train our cyber force to make them high value, high impact operators on the Joint battlefield. This requires innovative, agile learning mechanisms and modern facilities that place cyber technology and threats, and integration of cyber tradecraft advances and operational lessons learned on a more accelerated basis. It requires new talent management approaches to attract, screen, recruit and retain Soldiers and civilians with a high level of native cyber aptitude, and integrated approaches across cyber organizational structure, leadership training, and skills development.[27]

While what Major General Fogarty stated is true, there is a disconnect between the strategic ends and the lines of efforts associated with attaining the ends. That disconnect is where the strategy foreword discusses recruiting the best cyber workforce

to dominate in cyberspace, with no discernable line of effort associated with that goal. Successful performance in the cyber realm is largely dependent upon the recruitment of the right people with the right skills to realize the vision of cyberspace domination.

In DOD, resourcing can be typically tied to a line of effort within a strategy. If there is no line of effort tied to recruitment, then one could surmise that it may not have garnered the level of attention needed or it will not be provided additional resources and expected to fund out of current year or within the approved fiscal year defense plan. The counter to that argument is that it is not explicitly listed as a line of effort because the DOD, by individual Service, annually plans the number of personnel it will recruit is planned and programmed during the Planning, Programming, Budget and Execution process. With all of this said, the Army understands the need to recruit and train quickly.

The DOD has achieved some progress towards building cyber capacity and capability. It has recognized the need to consolidate comparable career management fields into one focused on cyber. The creation of a new Military Occupational Series to identify the elite group of cyber personnel and a Cyber Protection Brigade are just two indications of the fundamental transformations taking place.[28] The U.S. Cyber Command tasked each service to provide the 133 trained, staffed, and equipped cyber protection teams during the four-year phased implementation plan.[29] This meant force structure changes and rapid competency development is of strategic importance to ensure mission accomplishment. The DOD will review if additional compensation is necessary to recruit the best cyber warriors and civilians. The department currently offers recruitment and retention bonuses to certain career management fields.

Legislation may be needed to expand it to cyber forces, however, it is one of several approaches available to attract and recruit highly trained cyber professionals.

Words are important. This is highlighted to state that the words used do make a difference and sometimes focuses lines of effort where they need to be. For example, the strategy uses the words attract and recruit interchangeably, but they are different things. One could argue attracting is a step in the overall process of recruitment. Attracting a candidate is the “why” a potential recruit would want to work for DOD. Marketing your organization as the organization of choice is usually where the attraction lies for potential employees. That attraction can range from the core values an organization espouses to the balance sheets it publishes. In its attempt to attract potential recruits and civilians, DOD has developed several videos marketing directly to potential cyber warriors. The Army also utilizes social media to market why it is the employer of choice for cyber. Since cyber warriors tend to be familiar with computers and social media, it is a communication media that is deliberate and smart as this method reaches many potential candidates. The Society of Human Resource Management defines recruitment as the process of attracting individuals on a timely basis, in sufficient numbers and with appropriate qualifications, to apply for jobs with an organization.[30] Also within recruitment, the job analysis, screening of applicants, and selection portions are completed. Defining and understanding the meaning of these terms is important and can focus efforts to attracting Soldiers and civilians through a comprehensive recruitment strategy.

The National Institute of Standards and Technology, a sub-organization of the U.S. Department of Commerce, estimates that there will be a shortage of 1.5 million

cyber security personnel shortage by 2020.[31] This postulates that there are an insufficient number of trained cyber security personnel available and that the competition for resources will be that much more challenging. Added to this shortage is the fact that science, technology, engineering, and mathematics education statistics in the United States does not bode well in finding the talent necessary to build a formidable cyber force of the future. The National Science Foundation ranks the U.S. 8th graders 8th among the top 28 nations for proficiency in math and science.[32] This information is provided only to outline the challenges associated with building and maintaining a competent and capable cyber workforce.

Much more work is needed, but DOD is making strides towards the goal of building a cyber capacity quickly. In its cyber recruitment efforts, the Army is using assessments to determine cyber aptitude. For example, the Armed Services Vocational Aptitude Battery is an assessment that is used to determine aptitude for the cyber field. In addition, the Air Force, Navy, and Army are developing a joint computer-based "Cyber Test" to assess military applicants' propensity in a variety of computer and networking skillsets.[33] These assessments will provide an independent and objective measurement to gauge the type of individual with the propensity and aptitude to achieve in cyber thereby providing DOD with the requisite cyber ready forces it requires. There are some additional ways to recruit the necessary cyber forces quickly, but those will be discussed in the recommendations section of this paper.

Development

While recruiting the right people is extremely important to accomplishing the goals of the Army with regards to cyber, training enables that accomplishment. Training is central to the ability of DOD to dominate in the cyber domain. The Services have the

responsibility to man, train and equip, so I will discuss here how the Army and other Services can develop the cyber workforce the DOD needs. The Army predicates the training it delivers on the Army Learning Model. In 2011, the Army published the *U.S. Army Learning Concept* for 2015. This framework seeks to improve our learning model by leveraging technology without sacrificing standards so we can provide credible, rigorous, and relevant training and education for our force of combat seasoned Soldiers and leaders.[34] The *Army Learning Concept* 2015 is nested within our Army's framework of concepts. The core pillars of this framework are the *Army Capstone Concept*, the *Army Operating Concept*, the *U.S. Army Training Concept*, and the *Army Leader Development Strategy*. The Army Learning Concept recognizes and addresses the arrival of a new generation of Soldiers in our ranks who have grown up in a digital world.[35] The previous sentence confirms that the Army recognizes the need to have a more agile process for developing the training necessary to deliver highly trained cyber professionals at the right place and right time. However, the *Army Learning Concept* still bases the development of its instruction on the analysis, design, development, integration and evaluation (ADDIE) Model; although this model is very linear and the outputs from each phase must be approved prior to moving to the next phase.[36] The ADDIE model of instructional systems design was first developed for the U.S. Army during the 1970s by Florida State University's Center for Educational Technology.[37] ADDIE was later adapted for use by all branches of the U.S. Armed Forces. It has become a widely used and frequently modified best practice within the private sector. It is often employed for compliance training and other learning events that are not time sensitive.[38] The need to build a cyber capability quickly seems at odds with the

instructional design that is used to train cyber professionals. In the ADDIE model, each step has an outcome that feeds into the subsequent step.[39] The learning is based on a few factors like pre-determined course lengths, not synchronized to the individual learner, and focuses on how the instructor should lead the training to include time consuming and rigid development of the training in accordance with the ADDIE model.[40] Current instruction is based on individual tasks, conditions, and standards, which worked well when the Services had a well-defined mission with a well-defined enemy.[41]

Now and into the foreseeable future, the mission nor the enemy is well defined and some are willing to use their cyber capabilities to threaten the United States and its allies. This means the task, condition, and standard methodology may not be sufficient in the future. Fundamental changes in the instructional design would need to be considered if the effort to train cyber personnel rapidly and without a degradation in the quality of training is to be successful. The DOD should consider other models that are designed to ensure a much quicker analysis and development of the instructional material used to train our cyber professionals. Additionally, the ADDIE model has challenges in its need to be continuously adaptive in our learning culture.

The Army Learning Concept states that there are some challenges associated with the new learning concept.[42] One of those challenges is the concept of continuous adaptive learning model. This challenge simply states that the model must promote qualities in Soldiers and leaders and must be sufficiently adaptable to adjust to shifting operational environment demands.[43] If the ADDIE model is considered the gold standard, too rigid and linear, and mainly for instruction that is not time sensitive, then the Army may want to review and assess other instructional design models that is

based on the ever-changing environment. There is not much that DOD does that is not time sensitive. Therefore, it is imperative that we be innovative in our instruction, become more focused on the individual learning needs, and become more centered around training that incorporates students working together to construct knowledge from their collective experiences that reinforces engagement as well as retention of the material.

Institutional resourcing models designed for a peacetime force are not adaptive to the evolving needs of the Operational Army in an era of persistent conflict. The number of instructor contact hours drives the current resourcing model and is an obstacle to implementing any instructional strategy that is not face-to-face and instructor-centric. The current model incentivizes schools to maintain the brick and mortar mindset with a limited range of learning methodologies. In the current learning model, significant changes to learning programs require planning cycles of 3 to 5 years to implement, a timeframe that is not rapid enough to adapt to evolving operational demands. Well-designed learning must incorporate deliberate strategies to ensure learning transfers from the learning environment to the operational environment. Adapting to rapidly changing operations involves developing a deep understanding within specific content areas and making the connections between them.[44] That transferring learning to the operational environment was put to the test when DOD announced the Hack the Pentagon pilot program.

In 2016, the DOD hosted the Hack the Pentagon event. This event was designed to identify and resolve security vulnerabilities within Defense Department websites through crowdsourcing--is the first “bug bounty” program in the history of the federal

government. The Hack the Pentagon pilot program is modeled after similar challenges conducted by some of the nation's biggest companies to improve the security and delivery of networks, products and digital services; by providing a legal avenue for the responsible disclosure of security vulnerabilities; bug bounties engage the hacker community to contribute to the security of the Internet.[45] “This initiative will put the department's cybersecurity to the test in an innovative, but responsible way," Defense Secretary Ash Carter said of the program.”[46] "I encourage hackers who want to bolster our digital defenses to join the competition and take their best shot.”[47] The types of events help the Department improve its security posture while providing participants the experience that they otherwise would not have. The DOD should consider more training events like this to instill learning subsequently bolstering knowledge, skills, abilities needed to secure our networks, infrastructure, and the homeland.

Retention

The DOD strategy outlines the initiatives for recruiting and developing the cyber workforce and how the DOD will facilitate the joint forces resourcing changes now and into the future. However, it does not strategically discuss how it will retain this critical capability once recruited and trained. The Army has developed a Cyber Center of Excellence which is the premier cyber, signal and electronic warfare training a development in the Army, but no decipherable strategic method for retaining this talent once the significant investment has been made. The Services have had challenges challenge retaining young Captains and Majors. In November 2015, the Secretary of Defense Ashton Carter announced a strategic initiative called the Force of the Future. This initiative was designed to increase the permeability of new people and new ideas

to the DOD.[48] The initiatives outlined in the announcement memoranda are designed to put innovation in the forefront with the outcome of staying ahead of our competitors.

The initiatives were divided into military and civilian personnel initiatives that will provide the DOD with the skills needed to win in the cyber domain. Another term to describe the initiatives at a strategic level is talent management. What's absent is the strategy that outlines the ends, ways, and means balanced with appropriate risk. This is not to be critical, but when initiatives do not support an overall strategy, then they tend to fall flat since no one knows where they are going and how will they get there. Some of the initiatives are specifically aimed at retaining talent. In the cyber realm, this is of importance since the inventory and surplus are not congruent. Although those that are interested in working for the DOD because of the mission, ethos, esprit de corps, doing something that is meaningful and gives you sense of pride to serve the nation in and out of uniform, the realization is that not all that enter the cyber discipline are enamored with the aforementioned and feel they can get those same things outside of government or the military. Corporate organizations are willing to spend the six-figure salaries to get the cyber talent they require.

The competition for cyber talent is fierce. Even in a resource constrained environment, the DOD will need to address this in its strategy. Some of the initiatives that Secretary Carter outlines in his *Force of the Future* will require a change in legislation to implement, however, it is this level of innovation and strategic, critical, and creative thinking that is required to build and maintain a competent and capable cyber workforce. These are significant change management initiatives at their core and will require a focus on ensuring leaders are equipped to lead it. The DOD have very

structured and regimented cultures that do change on a dime and is difficult to change since it is a very bureaucratic and large organization. Culture will eat strategy for lunch every day if the leaders do not effectively manage it.[49] With this said, the DOD is on its way to building and maintaining a competent and capable cyber workforce. The OPM and DOD have announced several recruitment and retention flexibilities aimed at building and maintaining a cyber workforce. As mentioned previously, some of the proposed changes will require legislation changes, but there are some that do not and those should be able to move forward as soon as possible. However, like many things, flexibilities can be offered but that does not mean they will be used. Especially if you have leaders who do not strategically manage change and who are accustomed to doing things the same way with no regard for the evolving environment. You may also have leaders that simply do not know about how they can strategically recruit and retain a capable and competent cyber workforce.

In the next section of this paper I will offer some recommendations. Some of the recommendations are already in some form of progress but I want to emphasize that they are good ideas that should be capitalized on.

Recommendations

The DOD is on the cutting edge of technological change and it needs to be prepared to take on that challenge. The challenge to recruit, train, and retain highly trained cyber professionals remains a challenge for DOD and even the private sector. However, DOD has the wisdom and experience with dealing with these types of opportunities and will undoubtedly be successful. The DOD ultimately requires a new talent management strategy to address its issues in human resource management, but specifically cyber. With this said, there are more than a few initiatives that have been

announced by DOD that deserve the fullest attention to help them come to fruition. All the initiatives will require leaders that manage the change effectively. John Kotter put it best when he said, “Useful change tends to be associated with a multistep process that creates power and motivation sufficient to overwhelm all sources of inertia.”[50] Second, this process is never employed effectively unless it is driven by high quality leadership, not just excellent management.[51]

The Secretary of Defense outlined several of his initiatives under the *Force of the Future* and will be instrumental in recruiting, training, and retaining highly trained and qualified military and civilian cyber professionals. For example, a proposed recruitment flexibility for military personnel is the expanded lateral entry authority. This authority would allow experts and specialists in critical, high-skilled, and credentialed specialties to join the military at a mid-career level (Captain or Major) in the same manner currently authorized for medical officers, lawyers and chaplains; thereby increasing flexibility in recruiting experts in cyber who would otherwise be unlikely to assess into the military if required to enter at the most junior grades.[52]

Another proposal is a comprehensive review of DOD outreach programs that engage with America's youth and those who influence them, in their homes, schools, and communities. Those programs include: Junior Reserve Officer Training Corps, National Guard Youth Challenge, STARBASE, the Adopt-a-School Program, Civil Air Patrol, and Innovative Readiness Training. These programs display the myriad roles and missions of the Armed Forces and can be used to communicate the value and benefits of military service.[53] They require intermittent review to keep them relevant in this ever-evolving age of cyber. To meet the goal of maintaining a competent and

capable cyber workforce, then linking Force of the Future focus areas 1 and 2 together will afford a more balanced and comprehensive approach to recruiting the next cyber warriors and civilians.

Building on the previous proposal, the DOD should fully fund the Joint Advertising Marketing Research and Studies program. This program develops and executes a sustained advertising and marketing campaign aimed at connecting with and educating potential applicants, their influencers, and other members of the public about military service; building recognition of the "DOD Brand," and grow propensity to serve. DOD would customize and disseminate content through separate, but integrated print, TV, digital, and social media messaging that promotes the value and benefits of service, and synchronize the campaign with Military Service recruiting efforts.[54] As stated earlier in this paper, DOD needs to be able to reach younger audiences than it has traditionally been accustomed since the population of the United States is a lot more technically savvy. DOD may miss out if it does not adjust and develop programs where they begin recruiting earlier than high school.

Finally, the voluntary opt out of promotion cycle proposal is another legislative change, but it allows an officer to voluntary opt out of promotion boards that will allow them to undertake activities to deepen expertise or pursue enrichment activities.[55] This proposal would be very useful in retaining cyber warriors and can be used in conjunction with expanded training with industry opportunities. This effort would boost officer management flexibilities and force retention.

The DOD must also focus its efforts on building cyber capacity and capability in its civilian corps in conjunction with its efforts in the military. The *Force of the Future*

outlines some proposals that will facilitate civilian employee recruitment, training, and retention. A proposal that would require legislation is the ability to approve direct hiring authority for students and recent graduates.[56] This authority would allow the ability to hire students or recent graduates non-competitively and on the spot. Currently, if a recruiter meets with an undergraduate student, a graduate student, or recent graduate, the recruiter must direct the job seeker to the USAJOBS website to upload resume, transcripts, and any other relevant documents to begin the process of hiring; which could take anywhere from 90 days to 6 months to get an offer of employment.[57] As previously stated, the competition is tough for cyber talent and students simply cannot and will not wait that amount of time to get an employment offer. This is an authority that could boost capacity and capability quickly.

Another proposal is the establishment of a public-private talent exchange program.[58] This would authorize the creation of a two-way exchange program through which DOD and some of the America's best and most innovative private companies could temporarily exchange employees. The idea would be to share new ideas and state of the art best practices for mutual benefit to the government and industry.[59] Coupled with this program would be an expansion of the current military Training with Industry Program. Currently, it is extremely competitive and affords minimum amount of opportunities for many candidates. This program could be extremely valuable in building cyber capability quickly if more opportunities were available.

To build on the previous proposal, but focus internally, DOD should increase its use of rotational or developmental assignments for cyber professionals. The *Force of the Future* initiative states to leverage career broadening rotational programs such as

the White House Leadership Development Program and the Defense Senior Leader Development Program to increase number and quality of career broadening experiences available to civilians.[60] These are worthy and very competitive programs, however, in cyber, there's potential to build off of those programs and develop a cyber-specific program that would be developed jointly by CYBERCOM, Service specific cyber development institutions, and academia.

Conclusion

Recruiting, developing, and retaining highly skilled cyber professionals is a significant strategic challenge for the DOD. At the heart of this challenge is the development of a talent management strategy that outlines what the vision for the future, how DOD will get there (ways) and what will DOD use (means) to get to the endstate. The *Force of the Future* initiatives are a great start at the creative thinking that's necessary, but it needs to be rooted in an overall talent management strategy. The DOD will require a shift in its very regimented culture. As Dr. R. Craig Bullis stated to his U.S. Army War College Seminar 5 students, "Culture will eat strategy for lunch for every time."[61] This simply means the best laid strategy will not withstand a culture that is not adaptable and resistant to change. Change that is not lead with purpose with a discernable vision that is not communicated early and often is destined for failure. The DOD strategy outlined the need to build a capable cyber workforce with the requisite knowledge, skills, and abilities to successfully defend against cyber-attacks and protect valuable DOD information infrastructure. This mission is of utmost strategic importance if we are to protect and defend against cybersecurity attacks. These attacks are very different from what we have faced in state on state aggression. Cyber is being used to attack any vulnerability to U.S. infrastructure and networks and leaving them open to

attack from state and non-state actors is simply not responsible and can be extremely dangerous.

The DOD efforts in the *Force of the Future* are innovative on the surface, but requires successful implementation and institutionalization to gauge whether it is innovative. However, it is these types of initiatives and programs that will better enable the DOD to perform its mission effectively. Cyberspace is an extremely fluid domain to operate in and for the DOD to secure the Nation, it will require the same level of fluidity and adaptability in its personnel processes to achieve deterrence from and response to cyber-attacks. Recruitment is an important factor in achieving the strategic goal, but having the capacity without the appropriate capability (training) and platforms to prevent talent drain (retention) does little for the DOD. The *Force of the Future* initiatives, flexible instructional designs, and programs aimed at developing and retaining a cyber workforce from a strategic perspective will facilitate the recruitment, development, and retention of a competent and capable cyber workforce.

Endnotes

[1] Raymond T. Odierno, "CSA's Strategic Intent: Delivering Strategic Landpower in an Uncertain World," February 5, 2013, linked from the *U.S. Army Home Page,* https://www.army.mil/article/95729 (accessed April 1, 2017).

[2] U.S. Department of the Army, *The Operational Environment and Army Learning,* Army Training Circular 7-102 (Washington, DC: U.S. Department of the Army, November 2014), 1-1.

[3] U.S. Department of Defense, *DOD Cybersecurity Strategy* (Washington, DC: U.S. Department of Defense, April 2015), 2.

[4] International Telecommunications Union, "2016 ICT Facts and Figures," June 2016, linked from the *International Telecommunications Union Home Page*, http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (accessed February 11, 2017).

[5] Wikipedia, “Robert Tappan Morris,” https://en.wikipedia.org/wiki/Robert_Tappan_Morris (accessed April 1, 2017).

[6] Ibid.

[7] Ibid.

[8] John Markoff, “Computer Intruder is Found Guilty,” *New York Times Online,* January 23, 1990, http://www.nytimes.com/1990/01/23/us/computer-intruder-is-found-guilty.html.

[9] Brian Ries, “Hackers Most Destructive Attacks,” *The Daily Beast Online,* December 11, 2010, #3, http://www.thedailybeast.com/articles/2010/12/11/hackers-10-most-famous-attacks-worms-and-ddos-takedowns.html (accessed February 11, 2017).

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] Marina Koren, “About Those Fingerprints that Were Stolen in The OPM Hack,” *The Atlantic Online,* September 23, 2015, https://www.theatlantic.com/technology/archive/2015/09/opm-hack-fingerprints/406900/ (accessed February 12, 2017).

[14] Ibid.

[15] Barack Obama, *2015 National Security Strategy* (Washington, DC: The White House, April 2015).

[16] Ibid., 7.

[17] U.S. Department of Defense, *The Department of Defense Cyber Strategy* (Washington, DC: U.S. Department of Defense, April 2015), 2, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed April 1, 2017).

[18] Ibid.

[19] *The United States Strategic Command Home Page*, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/ (accessed February 12, 2017).

[20] Ibid.

[21] U.S. Department of Defense, *The Department of Defense Cyber Strategy.*

[22] Ibid., 3.

[23] Ibid.

[24] U.S. Department of Defense, "All Cyber Mission Force Teams Achieve Initial Operating Capability," *DOD News Online*, October 24, 2016, https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability (accessed March 31, 2017).

[25] Ibid.

[26] U.S. Department of Defense, *Mission Analysis for Cyber Operations of Department of Defense* (Washington, DC: U.S. Department of Defense, August 21, 2014), 9.

[27] U.S. Department of the Army, *U.S. Army Cyber Center of Excellence Strategic Plan* (Fort Gordon, GA: U.S. Department of the Army, September 2015), 1.

[28] U.S. Department of Defense, *Mission Analysis for Cyber Operations*, 13.

[29] U.S. Department of Defense, "All Cyber Mission Force Teams."

[30] Mryna Gustdorf, *Recruitment and Selection: Hiring the Right Person*, Staffing Management Instructors Manual (Alexandria, VA: Society for Human Resource Management, 2008), https://www.shrm.org/academicinitiatives/universities/TeachingResources/Documents/Recruitment%20and%20Selection%20IM.pdf (accessed February 1, 2017).

[31] *National institute of Standards and Technology Home Page,* https://www.nist.gov/ (accessed March 31, 2017).

[32] U.S. National Science Foundation, "How do U.S. 8th Graders Compare with Students in Other Countries in Math and Science?" linked from the U*.S. National Science Foundation Home Page* at "STEM Education Data," https://nsf.gov/nsb/sei/edTool/data/middle-07.html (accessed April 1, 2017).

[33] U.S. Department of Defense, *Mission Analysis for Cyber Operations*, 11.

[34] U.S. Department of the Army, *The Army Learning Concept 2015* (Washington, DC: U.S. Department of the Army, January 20, 2011), 1.

[35] Ibid., 1.

[36] U.S. Army Training and Doctrine Command, *Army Learning Policy and Systems*, TRADOC 350-70 (Fort Eustis, VA: U.S. Army Training and Doctrine Command, December 6, 2011).

[37] Ibid.

[38] Training Industry, "ADDIE Model," linked from the *Training Industry Home Page*, https://www.trainingindustry.com/wiki/entries/addie-model.aspx (accessed January 31, 2017).

[39] U.S. Army Training and Doctrine Command, *Army Learning Policy and Systems.*

[40] Ibid.

[41] U.S. Department of the Army, *Army Learning Concept 2015,* 7.

[42] Ibid.

[43] Ibid., 16.

[44] Ibis., 8.

[45] "Hack the Pentagon Pilot Program Opens for Registration," *DOD News Online*, March 31, 2016, https://www.defense.gov/News/Article/Article/710033/hack-the-pentagon-pilot-program-opens-for-registration (accessed February 10, 2017).

[46] Ibid.

[47] Ibid.

[48] U.S. Secretary of Defense Ashton Carter, "The Next Two Links to the Force of the Future," memorandum for Secretaries of the Military Departments, Washington, DC, June 9, 2016.

[49] Craig Bullis, *Organizational Culture and Leadership Lesson* (Carlisle Barracks, PA: U.S. Army War College, October 4, 2016).

[50] John Kotter, *Leading Change* (Boston: Harvard Business Review Press, 1996), 20.

[51] Ibid.

[52] Carter, "The Next Two Links to the Force of the Future," 2.

[53] Ibid.

[54] Ibid.

[55] Ibid., 1.

[56] Ibid.

[57] Ibid., 2.

[58] Ibid.

[59] Ibid., 5.

[60] Ibid.

[61] Bullis, *Organizational Culture and Leadership Lesson*.