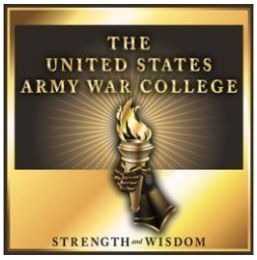
Strategy Research Project

DoD Strategy to Recruit, Train, and Retain Cyber-Ready Force

by

Lieutenant Colonel Marlyce K. Roth
United States Air Force

Under the Direction of:
Colonel Charles E. Grindle



United States Army War College
Class of 2016

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01-04-2016	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
DoD Strategy to Recruit, Train, and Retain Cyber-Ready Force

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Marlyce K. Roth
United States Air Force

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel Charles E. Grindle

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.
Please consider submitting to DTIC for worldwide availability? **YES:** ☐ **or NO:** ☒ **(student check one)**
Project Adviser recommends DTIC submission? **YES:** ☒ **or NO:** ☐ **(PA check one)**

13. SUPPLEMENTARY NOTES
Word Count: 5272

14. ABSTRACT
With the ever-growing cyber threat from state and non-state actors, U.S. national interests and those of U.S. allies are at a significant risk. Unlike the other domains, the cyber domain grows exponentially on a daily basis, so time is of the utmost importance for building and sustaining a cyber-ready force to protect against threats. The April 2015 DoD Cyber Strategy provides a solid foundation, for developing enterprise-wide programs and plans to build a cyber-ready force to meet the U.S. national military objectives that support the National Security Strategy.

15. SUBJECT TERMS
Domain

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	28	

DoD Strategy to Recruit, Train, and Retain Cyber-Ready Force

(5272 words)

Abstract

With the ever-growing cyber threat from state and non-state actors, U.S. national interests and those of U.S. allies are at a significant risk. Unlike the other domains, the cyber domain grows exponentially on a daily basis, so time is of the utmost importance for building and sustaining a cyber-ready force to protect against threats. The April 2015 DoD Cyber Strategy provides a solid foundation, for developing enterprise-wide programs and plans to build a cyber-ready force to meet the U.S. national military objectives that support the National Security Strategy.

DoD Strategy to Recruit, Train, and Retain Cyber-Ready Force

> The Director of National Intelligence named the cyber threat as the number one strategic threat to the United States, placing it ahead of terrorism for the first time since the attacks of September 11, 2001.
>
> —Department of Defense Cyber Strategy[1]

To address this threat, the Department of Defense (DoD) requires a highly skilled cyber force that can adapt quickly to rapidly changing capabilities. Additionally, this force needs to "ensure and enhance military capabilities in all domains, provide cyber options for the President, and to defend the nation against cyber attacks and cyber adversaries."[2] This paper focuses on the current cyberspace environment, the challenges associated with the DoD strategy to recruit, train, and retain a cyber-ready force, and the essential actions to address the fact that the DoD does not have the personnel necessary to create a safe and secure cyberspace environment for the United States and its allies. Operational design provides the framework that best addresses this complex issue and charts a path to the desired endstate.

Commanders identify and solve complex and ill-defined problems using operational design. Operational design provides the framework needed to understand the operational environment, to define the problem, and to develop an operational approach.[3] The operational approach provides "a description of the broad actions the force must take to transform current conditions into those desired at end state.[4] To understand the importance of a cyber-ready force and develop the operational approach to the way ahead, one must first understand the current cyber environment, which encompasses the threat landscape, the cyber mission, the DoD cyber strategy, and an analysis of the strategy.

Cyber Environment

Threat Landscape

Cyberspace touches every aspect of society: the economy, transportation, healthcare, the infrastructure, public safety, military, and national security. The United States extensive reliance on cyberspace provides many advantages and some disadvantages. The nation's ability to secure its assets (networks, weapon systems, infrastructure, etc.) and gain dominance in this domain benefits both the United States and its allies. Cyberspace has become vital to national security and economic prosperity.[5] However, "hostile actors use cyberspace as an asymmetric capability to strike the U.S. homeland and U.S. interests, directly and indirectly."[6] While the nation's cyber capabilities have expanded, the worldwide cyber threat is growing exponentially in scale and complexity. In addition, an increasing number of state and non-state actors are targeting United States and allied networks on a daily basis. Because cyberspace is so accessible, cyber threats range from state-sponsored offensive military operations and industrial espionage activities to non-state and Violent Extremist Organizations (VEO) designs to disrupt our way of life and criminal hackers seeking financial gain and attention. Additionally, even though U.S. cybersecurity teams can readily detect and defeat cyber attacks on the U.S. supply chain and critical infrastructure, attribution remains a significant challenge.[7] To address the cyber threat and assure the advantage in the domain, the DoD has specified several objectives to support the National Security Strategy (NSS).

Cyber Mission

Securing the cyber domain is an integral part of the U.S. military strategic objectives in several ways. First, to deter, deny, and defeat state adversaries, the DoD

must protect critical networks, weapon systems, and infrastructure. Second, to disrupt, degrade, and defeat VEOs using offensive cyber technologies, highly skilled personnel, and Tactics, Techniques, and Procedures (TTPs) to counter and disrupt their information and recruiting campaigns, their operations, their Command and Control (C2), and restrict their access to finances. Lastly, to strengthen the global network of allies and partners, the DoD must share cyber capabilities, information, and security practices.[8] To meet these objectives it is important to outline the cyberspace mission along with roles and responsibilities.

As part of the National Defense Authorization Act, the 2014 Cyber Mission Analysis specifies the DoD cyber mission is to: “secure, operate, and defend DoD networks; defend the nation in cyberspace; and support Combatant Command full spectrum operations in cyberspace.”[9] This mission enables the DoD to gain and maintain the advantage not only in cyberspace but also across the other four domains. U.S. Strategic Command (USSTRATCOM), as directed by the Unified Command Plan, has the responsibility for “synchronizing planning for cyberspace operations, in coordination with other combatant commands, the Services, and, as directed, other appropriate U.S. government departments and agencies.”[10] As a sub-unified command to USSTRATCOM, U.S. Cyber Command (USCYBERCOM) is responsible for the cyber mission and related USSTRATCOM responsibilities. The Cyber Mission Force (CMF) and DoD Information Network (DoDIN) forces carry out the cyber mission.[11]

In 2012, DoD built the CMF framework, which consists of 133 teams and approximately 6,200 military, civilian, and contractor personnel. This is a significant investment by the DoD and the United States. Strategically, the CMF framework

develops the goals and objectives of an offensive and defensive force to protect and defend U.S. national interests.[12] The CMF, which is to be fully manned, trained, and equipped by 2018, consists of Cyber Protection, National Mission, and Combat Mission forces. The Cyber Protection force has 68 teams that augment DoDIN forces assigned to defend DoD networks and systems. The National Mission Force (NMF) has 21 teams that defend the United States and its interests against strategic cyber-attacks. The Combat Mission force has 44 teams that support combatant commands in carrying out plans and operations to create cyberspace effects.[13] The Cyber Protection and Combat Mission teams support the combatant command plans and operations, while the NMF supports USCYBERCOM. The teams also support other national mission requirements as directed.[14] Although military personnel, government civilians, or contractors can support this mission, there are certain elements of the mission that require a uniformed cyber force.

There are many similarities between cyber personnel roles in industry and those in the U.S. military. Therefore, some observers have questioned the need for uniformed cyber forces. The United States needs a uniformed cyber force for the following reasons:

- *Integration of Cyber Capability into Full Spectrum Operations.* Since cyberspace operations are part of full spectrum operations, uniformed cyber personnel are part of the chain of command in order to support these operations.[15]

- *Authority to Operate in Cyberspace.* Title 10 and Title 50 of the U.S. Code govern military and national defense activities. DoD personnel are required to conduct certain activities under Title 10, which also prohibits them from engaging in other types

of activities. Legal boundaries are even more complex when cyber operations engage in a stand-alone conflict or serve as part of broader hostilities. In this situation, questions arise regarding the law of armed conflict and the status of participants as legal combatants. Only uniformed cyber warriors can participate as legal combatants.[16]

- *Deployability.* Currently, when the U.S. military deploys, varying parts of the networks deploy with them. Depending on what systems and services are in the theater, uniformed network operators and defenders must also deploy. At certain levels, deployed cyber forces can include civilians or contractors; however, this is not the case at the lower levels. Cyber personnel at the lower levels must be military for the following reasons: they routinely integrate into operations; they deploy in accordance with military orders; they have clear roles in the military chain of command; they are trained and equipped for combat.[17]

The DoD cyber mission is best fulfilled with a force that includes military personnel, government civilians, and contractors to appropriately execute given authorities. While the services are eager to outsource and provide reach-back for as many network services as possible, the need for uniformed personnel to deploy and enable the connectivity to reach-back locations is vital. Additionally, Joint Force Commanders will want assured access to network services if connectivity to reach-back sites is lost. This requires having a small footprint of equipment and skilled personnel in the area of responsibility to provide these services. No matter what force combination is used, recruiting, training, and retaining, a qualified cyber workforce is a challenge for the DoD. The DoD strategy to meet this challenge has recently been published.

DoD Cyber Strategy

DoD developed the following strategy in 2015 to build, maintain, and sustain a ready force to conduct cyberspace operations.

> To make good on DoD's significant investment in cyber personnel, and to help achieve many of the objectives in this strategy, DoD's first priority is to develop a ready Cyber Mission Force and associated cyber workforce. This workforce is built on three foundational pillars: enhanced training; improved military and civilian recruitment and retention; and stronger private sector support.[18]
>
> *Maintain a persistent training environment.* DoD requires an individual and collective training capability to achieve the goals outlined in this strategy and to meet future operational requirements. U.S. Cyber Command will work with other components, agencies, and military departments to define the requirements for and create a collaborative training environment. This will enable the total cyber force to conduct joint training (including exercises and mission rehearsals), experimentation, certification, as well as the assessment and development of cyber capabilities and tactics, techniques, and procedures for missions that cross boundaries and networks.[19]
>
> *Build viable career paths.* Throughout the course of this strategy, and following the CMF decisions of 2013, DoD will continue to foster viable career paths for all military personnel performing and supporting cyber operations.[20]
>
> *Draw on the National Guard and Reserve.* Throughout the course of this strategy, DoD will draw on the National Guard and Reserve Components as a resource for expertise and to foster creative solutions to cybersecurity problems. The Reserve Component offers a unique capability for supporting each of DoD's missions, including for engaging the defense industrial base and the commercial sector. It represents DoD's critical surge capacity for cyber responders.[21]
>
> *Improve civilian recruitment and retention.* In addition to developing highly skilled military personnel, DoD must recruit and retain highly skilled civilian personnel, including technical personnel for its total cyber workforce. Civilians must follow a well-developed career development and advancement track and be provided with best-inclass opportunities to develop and succeed within the workforce.[22]
>
> *Develop and implement exchange programs with the private sector.* To supplement DoD's civilian cyber workforce, DoD must be able to employ technical subject matter experts from the best cybersecurity and

> information technology companies in the country to perform unique engineering and analytic roles within DoD. The Defense Department will implement successful private sector exchange programs to bring measurable benefits to the Department of Defense through the design and development of new operational concepts for DoD's cyberspace missions.[23]
>
> *Support the National Initiative for Cyberspace Education.* DoD will develop policies to support the National Initiative for Cybersecurity Education. Working with interagency partners, one or more educational institutions, as well as state and private sector partners, DoD will continue to support innovative workforce development partnerships focused on both the technical and policy dimensions of cybersecurity and cyber defense.[24]

The DoD cyber strategy provides only a broad brush of what needs to be done to recruit, train, and retain a cyber-ready force. Analysis of the strategy reveals several issues to address in order for the strategy to succeed.

Strategy Analysis

Recruiting of cyberspace professionals into DoD, will present multiple challenges. The first is the fact that cyberspace personnel require wide-ranging skill sets that take years to acquire and sustain.[25] It is difficult to recruit qualified cyberspace professionals with the required skillsets so that they can hit the ground running. Figure 1 broadly depicts the skills required to operate in the cyberspace domain. While a single individual does not need all of these skillsets, recruiting candidates with the expertise and the proper certifications in any of these broad areas is challenging.

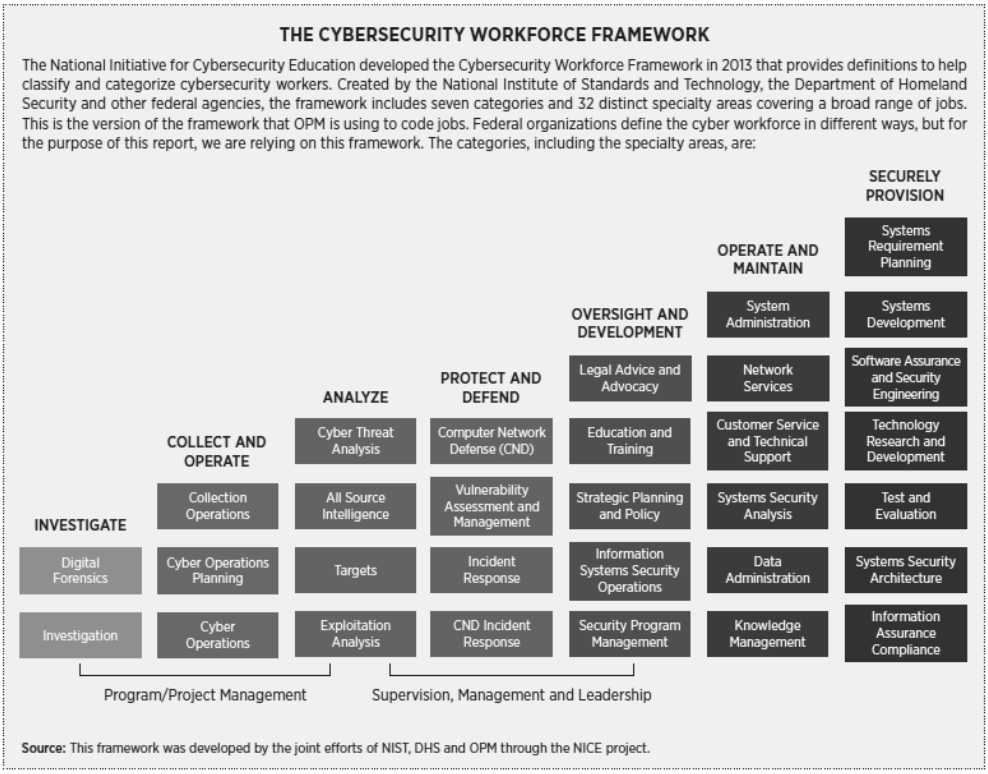


Figure 1: Required Skillsets[26]

The second challenge is DoD's ability to compete with the private sector in recruiting skilled cyber personnel. The private sector also has a high demand for these personnel; it can offer higher wages and incentives than the DoD can. According to the Bureau of Labor Statistics, estimates show that by 2018, 4.6M IT personnel will be required to support the commercial sector.[27] Figure 2 shows the results of a 2015 Computerworld salary survey that compares the salaries (Base + BAH) of military personnel with those of their civilian counterparts. These results are telling, especially at the lower pay grades where most of the cyberspace workforce resides. As this compensation gap widens, the DoD will continue to fall behind in recruiting the needed skilled workforce. Additionally, DoD is competing with other government agencies for the same pool of people. Admiral Michael Rogers, Chief of CYBERCOM, explains how

the DoD must compete with the private sector: "We are not going to compete on the basis of money. Where we're going to compete is the idea of ethos, culture that you're doing something that matters, that you're doing something in the service of the nation."[28]

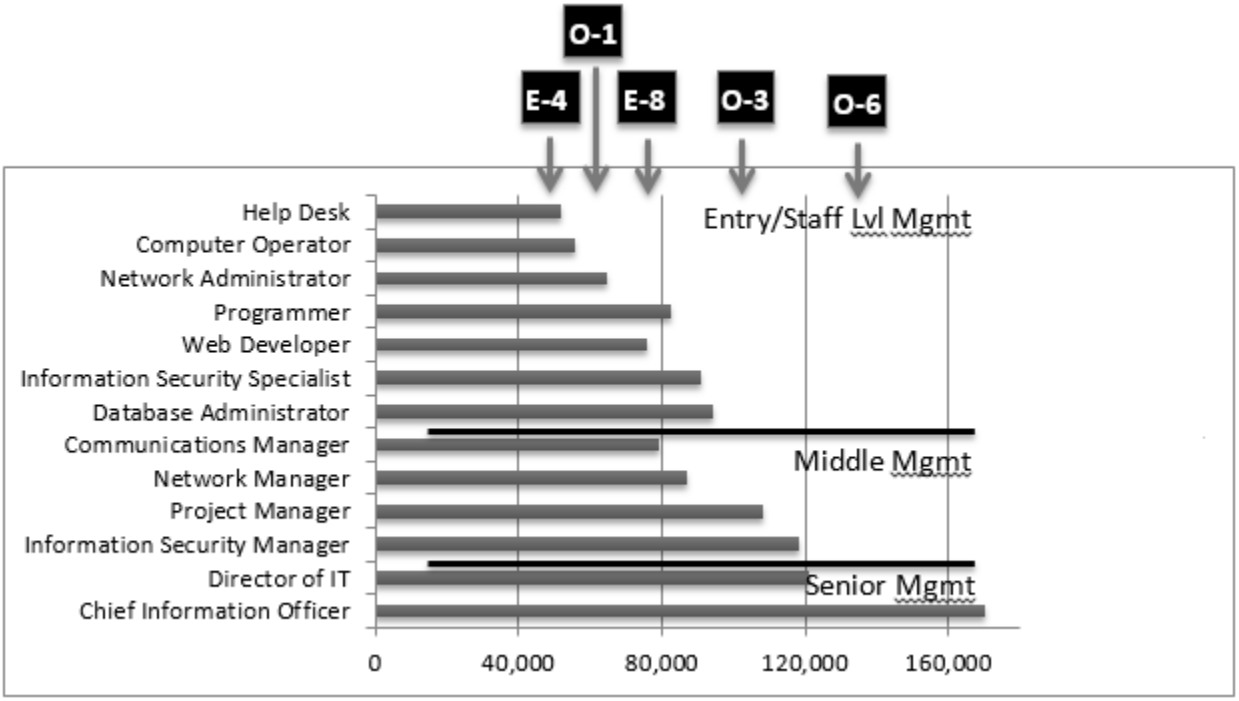


Figure 2: Salary Comparison[29]

The third challenge is that the DoD will not be able to meet CMF recruiting requirements without leveraging the total force in addition to new recruits from the public sector. The commander of CYBERCOM is working with Services Components, National Guard Bureau and Reserve Chiefs to arrive at a total force solution.[30] The services are working hard to recruit from the active and reserve forces to leverage personnel who are already available for service, who have acquired basic service training, and who have the aptitude to operate in the cyber domain.

The forth challenge comes from two key barriers to entry into the DoD. First, the federal government's stringent security clearance requirements and approval timelines

eliminate some promising candidates and discourage others. Second, outdated and complex personnel rules have hindered DoD's ability to compete in a timely manner for a limited talent pool more difficult.[31] To address these barriers, DoD leaders must eliminate bureaucratic complications and expedite the hiring process, especially for cyber personnel.

The fifth challenge is to collaborate with private sector companies to develop an exchange program. This would be beneficial, as the program allows both DoD and private companies to leverage one another's personnel and expertise. Additionally, the program will enable cyber personnel to gain experience and training that they may not receive from their respective organizations.

Finally, the sixth challenge is DoD's adoption of other recruiting options such as scholarships, marketing campaigns, and entry at higher rank levels based on expertise and experience. While the DoD previously offered an Information Assurance Scholarship Program, it has not been funded for the past two years.[32] The Air Force and Army states the importance of cyber expertise in their recruiting commercials, but Raytheon found in an October 2015 survey that cyber educational opportunities are scarce and that information on the importance of cyber skills and the opportunities available are not reaching the millennial's.[33] The Navy is offering some enlistees with a cyber background entry in as E-4's with a six-year enlistment.[34] Unlike other domains, the technology used in the cyber domain changes daily. To maintain an advantage in the domain, the DoD's cyber force has to adapt quickly so on-going training is essential the cyber workforce.

The commander of USCYBERCOM, Admiral Rogers asserts “DoD must continue learning and developing new skills and techniques just to tread water, given the rapid pace of change in cyberspace.”[35] To remain competent, cyber personnel require wide-ranging skill sets that take several years to acquire and daily use and training to sustain.[36] At this time, the services are working independently to train the DoD cyber force. The Army has an Information Technology schoolhouse, but it focuses mainly on cybersecurity and managing cyberspace capabilities, not on cyber operations. The Air Force maintains an Information Operations schoolhouse, and Air Force leaders are working to incorporate cyber training into its curriculum. The Navy provides cyber-related training at its Center for Information Dominance.[37]

While each of the services relies on schoolhouses and programs to train their personnel, DoD’s diminishing budgets and declining personnel strength levels, along with network consolidations, require the development of efficiencies in DoD’s cyber training efforts. Developing a joint cyber schoolhouse will not only create efficiencies it will also enhance the effectiveness and agility of the cyber force by combining the best training methods and materials of each service. Additionally, collaboration with other government agencies and the private sector (universities and companies) to develop and share educational opportunities will gain efficiencies through sharing resources and will enhance the capability and readiness of the cyber force by leveraging expertise.

Training of CMF teams is DoD’s current focus, but sustainment of training for the DoDIN military and civilian workforce is also important. One of the three cyberspace missions is to execute DoDIN operations. The other two missions call for executing Defensive Cyber Operations and Offensive Cyber Operations, which are CMF

responsibilities. “DoDIN Ops include designing, building, configuring, securing, operating, maintaining, and sustaining the information environment that we rely on for operations.”[38] Since the consolidation of Air Force networks and the movement of boundary and core service system administration to the integrated-network operations security centers, network administrators at the base level do not receive any training beyond what is provided at technical schools. For promotion purposes, Airmen must pass annual tests on the operation of their equipment, but they have no access to the equipment in order to conduct hands-on training. Additionally, these network administrators are responsible for administering equipment at a deployed location, but don’t have the authorization to administer equipment in garrison. Before deployment, they receive approximately two-weeks just-in-time training. However, as anyone in the cyber domain knows, this is not nearly sufficient to maintain proficiency on any system in which technology (hardware, software) changes rapidly. The client technicians have been able to maintain their proficiency as they operate and fix the client systems on a daily basis, but they too require periodic training on the latest technology. The Navy and Marines have also consolidated their networks and are dealing with the same issues as the Air Force. The Army has a plan in place to begin consolidating its network, but the timeframe has yet to be determined. While efficiencies in manpower, equipment, and maintenance can be gained by consolidating networks, the DoD must ensure that effectiveness and timeliness of services and support is at least equal or better than it was prior to consolidation. Otherwise, operational effectiveness will suffer. Furthermore, as the military is moving access of network and core services (e-mail, portal) from the cloud, there is no assurance that every deployed location will have immediate and

sustained access to these cloud services. Therefore, the need for military members to maintain proficiency training in support of DoDIN operations both in-garrison and deployed is vital. DoD's significant investment in training a cyber force necessitates a strategy to retain that force.

As is the case with recruitment, the challenges of wages, collaboration with private sectors, and incentives (promotions on technical vs. military skills, pay, bonuses, etc.) are critical for retaining a cyber-ready force. While the services should be able to recruit and/or realign the manpower required to build the 133 CMF teams and sustain DoDIN operations, retaining this manpower will be more challenging. DoD cyber force retention issues begin with the lack of promotion opportunities for technical personnel and the fact that they can earn more in the private sector.[39]

The consolidation of Air Force networks has eroded the morale of the DoDIN operations workforce, mainly network administrators, and hastened their departure from the Air Force. Personnel at the base level have lost most of their administrative privileges and thus are losing their expertise; they have little motivation to come to work or stay in the service. They can join the private sector work force, earn higher salaries, and hone their skills to be productive employees. Understanding and analyzing the current cyber threat environment and DoD's strategy to recruit, train, and retain a cyber-ready force are fundamentally important for countering the threat and building a cyber-ready force to maintain an advantage in the cyber domain. Defining the problem and devising an operational approach to solve it—these are still the challenges.

Problem

DoD does not have the personnel to build, maintain, and sustain the CMF and DoDIN force needed to carry out the DoD cyber mission and achieve national military objectives. The combined service percentage of available trained personnel to fill the 133 CMF teams currently lags at 54%. The individual service percentages of personnel trained to date vs. those required to meet full team strength are as follows: Army 64%, Air Force 44%, Navy 56%, Marines 43%. DoD directed the services to have the 133 teams fully operational by 2016. Nevertheless, due to recruiting and training issues, the deadline is now 2018. In addition, there is no guarantee the services will meet this date.[40] These numbers do not include the manning required to support DoDIN operations. While there is no documented issue regarding manning levels to support DoDIN operations, personnel in this mission area still require extensive technical skill sets. Recruiting, training, and retaining DoDIN operators competes with the CMF requirement, so DoD's ability to maintain adequate manpower for the DoDIN mission will be a continuing issue. The operational approach enables personnel and cyber leaders to address the cyber threat and the lack of a cyber-ready force.

Operational Approach

The operational approach promotes unity of effort in the interorganizational environment. It enables DoD leaders to establish, develop, and sustain a cyber-ready force to achieve the endstate of a secure and stable cyberspace environment. Interorganizational partners in this endeavor include DoD; U.S. government and state agencies; foreign military forces and their government agencies; intergovernmental organizations; and the private sector.[41] Figure 3 depicts a viable operational approach. The Lines Of Effort (LOE) include recruiting, training, retaining, collaborating and

information sharing and funding, which provide essential ways for achieving the stated endstate. The recommended tasks to carry out each LOE follow:

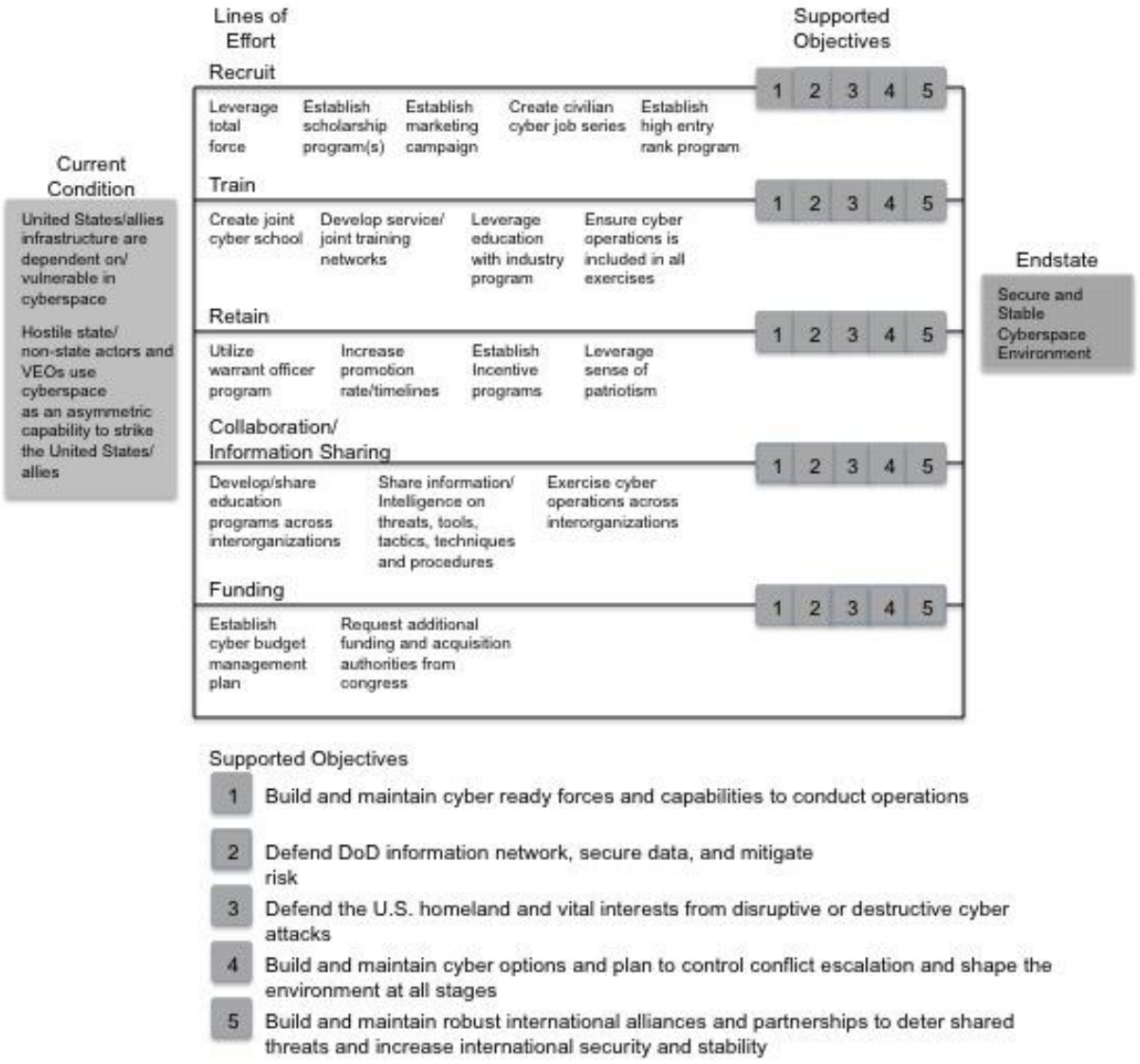


Figure 3: Operational Approach for Building a Cyber-Ready Force[42]

Recruit

There are several ways to recruit a cyber-ready force: First, leverage the total force. The Air Force and Army are already leveraging Reserve and Guard forces to fill their cyber team requirements.[43] Other total force options may entail creating a cyber

reserve corps, like the military's Reserve Officer Training Corps (ROTC). This option would encourage more college students to consider government service.[44] Additionally, the services can cross-train uniformed personnel from other career fields.

The second way to increase the pool of cyber talent is to offer undergraduate and graduate scholarships to students in the cybersecurity, science, technology, engineering, and mathematics fields. Scholarships provide several benefits in recruiting college students. Scholarships require a post-graduation service commitment—or reimbursement if individual defaults on their obligation. This assists DoD in identifying the number of individuals they have in the pipeline, and the commitment enables these candidates to begin the lengthy security clearance process to ensure they can begin work immediately upon graduation. Some scholarships also allow the DoD civilian hiring authorities to exercise excepted service appointing authority. This process bypasses bureaucratic hiring delays that are a significant source of frustration for candidates and hiring managers alike.[45]

The third tool to enhance recruiting is marketing. DoD needs to work with Silicon Valley companies and universities to develop cyber specific courses (cybersecurity, digital forensics, network administration and engineering, etc.) that educate college students in the cyber fields needed to meet both private and federal IT and cyber requirements. Additionally, the DoD needs to develop a cyber marketing campaign that facilitates contact between cyber professionals and students at university career fairs or other forums. These activities provide recruiters and ROTC detachments with marketing information on the cyber career fields, publicizing opportunities and stressing their importance to the nation's welfare. Finally, the marketing campaigns need to leverage

individual's sense of patriotism and with their service they are supporting something larger than themselves.

The fourth recruiting enhancement pertains to the DoD civilian force. Using data from the Office of Personnel Management and the National Initiative for Cybersecurity Education, the White House cybersecurity coordinator should examine the current cyber workforce and the required capabilities, then develop a strategy to meet future needs. This strategy should include development of a new civilian occupational job series for the cyber workforce. This entails development of position descriptions with the current skillsets required. This kind of specificity will enable hiring authorities and recruits to identify what positions best fit their needs and talents. Currently, most of the civilian cyber force serves under the General Schedule (GS) 2210–Information Technology Management Series. The civilian manning system designates 11 different specialties, and eight other GS series cite IT and cyber-type specialties. This lack of consolidation makes it difficult for those entering the federal cyber workforce to know where their jobs are located, and they do not have a clear career path to support their development and promotions. The Cybersecurity Workforce Framework in Figure 1 can be a baseline to develop the new cyber job series.[46]

The final recruiting recommendation is to establish an opportunity for cyber personnel to enter the military workforce at higher than standard entry-level ranks. Similar to the medical field, DoD should allow potential enlistees and officers to enter the military at higher ranks based on their experience, certifications, and education levels. This would provide a great incentive, especially for young college students. After cyber recruits enter the DoD, training them is the next critical step.

Train

Cyberspace is a rapidly changing environment in both its physical systems and infrastructure and in the TTPs needed to manage and defend those systems and infrastructure and to conduct offensive operations. To gain efficiencies and enhance security, the DoD is consolidating networks and standardizing architectures. As the DoD is moving to a joint information environment, its training should account for this. DoD should create a joint cyber schoolhouse to provide standardized training to CMF teams and DoDIN operators and administrators. Of course, each service has unique missions that require more specified training. Therefore, after cyber personnel have completed their standardized training, they can enter into their service specific training. In the services that have consolidated their networks, there is a need for the development of service and/or joint training networks for administrators. Administrators require hands-on training with equipment and capabilities that they no longer have access to since the network consolidation and standup of the enterprise service desks. The training also enhances administrators' troubleshooting skills and keeps their skill sets current. If personnel do not have the ability to train daily on their skill sets, they will put the DoD at a significant disadvantage when they are tasked to support in garrison and deployed requirements. Just-in-time training does not allow for the development and sustainment of troubleshooting and highly technical skills. DoD can also leverage the education-with-industry program to develop and enhance cyber personnel skillsets. This program provides hands-on educational experience to give DoD personnel management and technical skills as they study best practices with leaders of industry. Most importantly, cyber training and TTPs must be evaluated continuously; DoD must ensure cyber

operations are part of all exercises. All the training and exercises are for naught if the DoD cannot retain these highly skilled cyber personnel.

Retain

While it is difficult for DoD to compete with private industry in salaries and benefits, possibly a combination of monetary and promotion incentives, besides leveraging their sense of patriotism, will enable the DoD to retain more of their cyber force. Regarding promotions, services can utilize the warrant officer program to provide an incentive for entry-level and mid-level personnel. Additionally, services can consider increasing promotion rates or expediting promotions for cyber personnel. From the monetary perspective, services can evaluate providing enlistment bonuses and special duty pay for critically manned military cyber fields. For civilians, expansion of the special or additional pay program to all cyber-related job series could provide incentive for civilians to either stay in the cyber fields or move to them. Even if DoD builds the cyber-ready force it needs, it should also build and maintain robust alliances and partnerships to deter shared cyber threats to increase international security and stability.[47] The goal of creating a secure and stable cyber environment requires collaboration and information sharing with interorganizational partners.

Collaboration and Information Sharing

Consider the following recommended LOE to support collaboration and information sharing with interorganizational partners. First, DoD should develop and share cyber education programs. Second, DoD should share information and intelligence on threats, tools and TTPs. Lastly, to the fullest extent possible; DoD should include interorganizational partners in exercises. To support the DoD cyber strategy and

the operational approach depicted in Figure 3, management of the cyber budget must be improved.

Funding

As noted in the DoD cyber strategy, “cyber funding is spread across the DoD budget, to include the Military Intelligence Program, in multiple appropriations, budget lines, program elements, and projects.”[48] Additionally, the DoD garners funding from the National Intelligence Program to support cyber missions. This dispersed budgeting challenges DoD’s management of the cyber force. To improve the efficiency and effectiveness of the cyber mission and gain efficiencies in management, the DoD must develop a budget management plan.[49] This plan should not only synchronize funding sources but should also specify DOD priorities and show how they support interorganizational partners. With heightened awareness of the cyber threat and with an effectively managed cyber budget, requests for additional funds from Congress will be easier to justify and articulate. Additionally, given the urgent need to acquire the latest technology and recruit sufficient, well-trained cyber personnel, DoD should request new acquisition authorities from Congress to expedite purchasing of capabilities and to facilitate acquiring cyber talent. While there are no assured ways to recruit, train, and retain a cyber-ready force, the operational approach above provides a promising way ahead to meet this need.

Conclusion

As the Director of National Intelligence declared, the cyber threat is the gravest strategic threat to the United States.[50] Additionally, the cyberspace strategic environment is changing quickly, but there are no globally agreed-upon rules of engagement. To address this threat, the DoD must operate dynamically, flexibly, and

agile in the cyber domain. Furthermore, DoD must anticipate developing cyber threats, identify new capabilities, and ascertain how to improve partnerships and planning with interorganizational partners. These tasks cannot be accomplished without the men and women of the DoD, who are the DoD's greatest strength and source of inspiration.[51] DoD is not only concerned about the ability to recruit, train, and retain qualified uniformed and civilian personnel to support current and future cyber operations, but also with how mission-readiness in the cyber domain is impacted by protracted hiring timelines, security clearance processing, and training requirements.[52] The April 2015 DoD Cyber Strategy provides a solid foundation for the development of enterprise-wise programs and plans to develop and maintain a cyber-ready force to meet the U.S. national military objectives in support of the NSS. This strategy, however, does not provide a detailed outline of the programs or policy changes needed to meet the strategy goals. The details needed to build on this foundation still have to be developed. This can be done through coordination among the White House Cybersecurity Coordinator, DOD, other federal agencies, and private sector companies and universities. While some realignment of programs and policies are workable, most require sufficient and sustained funding from Congress to implement. Without this funding, DoD will not be able to meet national and military objectives. The operational approach in Figure 3 provides a detailed way ahead to meet the strategic goals and endstate of a secure and stable cyberspace environment, but to be successful, DoD must obtain funding and implement the approach in a coordinated and timely manner. The current cyber budget line of $7 billion in 2017 and almost $35 billion over the next five years provides a good baseline for achieving the goals and endstate.[53] With the

ever-growing cyber threat from state and non-state actors, U.S. national interests and those of U.S. allies are at a significant risk. Unlike the other domains, the cyber domain grows exponentially on a daily basis, so time is critical. Now is the time for building and sustaining a cyber-ready force to protect against current and future threats.

Endnotes

[1] Ashton B. Carter, *The Department of Defense Cyber Strategy* (Washington, DC: U.S. Department of Defense, April 2015), 9.

[2] U.S. Department of Defense, *Mission Analysis for Cyber Operations of Department of Defense* (Washington, DC: U.S. Department of Defense, August 21, 2014), 6, https://publicintelligence.net/dod-cyber-mission-analysis/ (accessed October 27, 2015).

[3] U.S. Joint Chiefs of Staff, *Joint Operation Planning*, Joint Publication 5-0 (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011), III-15; Carter, *The Department of Defense Cyber Strategy,* xix, xxi.

[4] Ibid., GL-13.

[5] Therese Delpech, "Space and Cyberdetterence," in *Nuclear Deterrence in the 21st Century* (Santa Monica, CA: Rand Corporation, 2012), 151, http://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1103.pdf (accessed October 1, 2015).

[6] U.S. Department of Defense, *Mission Analysis for Cyber Operations of Department of Defense,* 6.

[7] Admiral C.D. Haney, *Statement of Admiral C.D. Haney, Commander, United States Strategic Command, Before the Senate Committee on Armed Services,* Posture Statement (Washington, DC: U.S. Department of the Navy, February 27, 2014), 2, https://fas.org/irp/congress/2014_hr/022714haney.pdf (accessed October 27, 2015).

[8] U.S. Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2015* (Washington, DC: U.S. Joint Chiefs of Staff, June 2015), 7-9.

[9] U.S. Department of Defense, *Mission Analysis for Cyber Operations of Department of Defense,* 8-9.

[10] Ibid.

[11] Ibid.

[12] Carter, *The Department of Defense Cyber* Strategy, 6.

[13] U.S. Department of Defense, *Mission Analysis for Cyber Operations of Department of Defense,* 9-10.

[14] Carter, *The Department of Defense Cyber* Strategy, 6.

[15] Christopher Paul, Isaac R. Porche III, and Elliot Axelband, *The Other Quiet Professionals, Lessons for Future Cyber Forces from the Evolution of Special Forces* (Santa Monica, CA: RAND Corporation, September 23, 2014), 26, https://www.rand.org/content/dam/rand/pubs/research_reports/RR700/RR780/RAND_RR780.synopsis.pdf, (accessed October 27, 2015).

[16] Ibid., 27.

[17] Ibid.

[18] Carter, *The Department of Defense Cyber* Strategy, 17.

[19] Ibid.

[20] Ibid., 18.

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] Ibid.

[25] Paul, Porche, and Axelband, *The Other Quiet Professionals*, 34.

[26] Booz Allen Hamilton, "Cyber In-Security II: Closing the Federal Talent Gap," April 2015, 8, http://www.boozallen.com/insights/2015/04/cyber-in-security-closing-the-federal-talent-gap, (accessed on November 28, 2015).

[27] U.S. Department of Defense, *Cyber Operations Personnel Report* (Washington, DC: U.S. Department of Defense, April 2011), 8, http://www.nsci-va.org/CyberReferenceLib/2011-04-Cyber Ops Personnel.pdf (accessed November 27, 2015).

[28] Andrew Tilghman, "Cyber Force Grows, Along with Retention Concerns," *Military Times Online*, March 16, 2015, http://www.militarytimes.com/story/military/careers/2015/03/14/cyber-growing/70210162/, (accessed November 27, 2015).

[29] Computerworld, "IT Salary Survey 2015," http://www.computerworld.com/category/salarysurvey2015/ (accessed November 27, 2015); Defense Finance and Accounting Services, *2015 Military Pay Chart* (Washington, DC: U.S. Department of Defense), http://www.dfas.mil/dam/jcr:b6ef41d4-f071-45f9-b863-70b202be05a6/2015MilitaryPayChart_2.pdf (accessed November 27, 2015).

[30] Admiral Michael S. Rogers, *Statement of Admiral Michael S. Rogers, Commander, United States Cyber Command, Before the Senate Committee on Armed Services*, Posture Statement (Washington, DC: U.S. Department of the Navy, March 19, 2015), 7, http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-19-15.pdf (accessed October 27, 2015).

[31] Hamilton, "Cyber In-Security II," 3.

[32] Ibid., 12.

[33] National CyberSecurity Alliance, *Securing our Future: Closing the Cybersecurity Talent Gap* (Essex, UK: Raytheon, October 2015), 8, http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_278609.pdf (accessed on November 27, 2015).

[34] Andrew Tilghman, "As Cyber Force Grows, Manpower Details Emerge," *Military Times Online*, September 23, 2014, http://www.militarytimes.com/story/military/pentagon/2014/09/23/as-cyber-force-grows-manpower-details-emerge/16097651/, (accessed November 27, 2015).

[35] Rogers, *Statement of Admiral Michael S. Rogers, Commander, United States Cyber Command, Before the Senate Committee on Armed Services*, 13.

[36] Paul, Porche, and Axelband, *The Other Quiet Professionals*, 34.

[37] Ibid., 33-34.

[38] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly* 73 (Second Quarter, 2014): http://ndupress.ndu.edu/News/NewsArticleView/tabid/7849/Article/577499/jfq-73-the-joint-force-commanders-guide-to-cyberspace-operations.aspx, (accessed December 11, 2015).

[39] Paul, Porche, and Axelband, *The Other Quiet Professionals,* 35.

[40] Bill Matthews, "Military Battles to Man its Developing Cyber Force," *GovTech* Works, September 16, 2015, https://www.govtechworks.com/military-battles-to-man-its-growing-cyber-force/#gs.fACa3Io (accessed October 27, 2015).

[41] U.S. Joint Chiefs of Staff, *Interorganizational Coordination during Joint Operations,* Joint Publication 3-08 (Washington, DC: U.S. Joint Chiefs of Staff, June 24, 2011), x.

[42] U.S. Joint Chiefs of Staff, *Joint Operation Planning*, 7-8.

[43] Matthews, "Military Battles to Man its Developing Cyber Force."

[44] Hamilton, "Cyber In-Security II," 13.

[45] Ibid., 10-11.

[46] Ibid., 6, 9.

[47] Carter, *The Department of Defense Cyber Strategy*, 8.

[48] Ibid., 30.

[49] Ibid.

[50] Ibid., 9.

[51] Ibid., 33.

[52] U.S. Department of Defense, *Cyber Operations Personnel*, 40.

[53] Aaron Mehta, "Carter Unveils Budget Details; Pentagon Requests $582.7 Billion," *Defense News*, February 2, 2016, http://www.defensenews.com/story/breaking-news/2016/02/02/carter-unveils-budget-details-pentagon-requests-5827b-funding/79686138/, (accessed February 10, 2016).