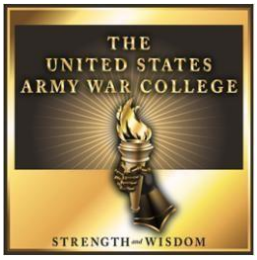
Strategy Research Project

Putting the Pieces Together: Army Cyber Warrior Talent Management

by

Colonel Calondra L. Fortson
United States Army

Under the Direction of:
Colonel Charles E. Grindle



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
Putting the Pieces Together: Army Cyber Warrior Talent Management

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Calondra L. Fortson
United States Army

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.
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:** ☒ **Mentor:** ☒

13. SUPPLEMENTARY NOTES
Word Count: 7,722

14. ABSTRACT
Cyberspace operations are critical to the success of the Department of Defense's (DoD) mission in a volatile, uncertain, complex and ambiguous multilateral world. Just as the United States envisions major armed conflict, cyberspace operations are an existential risk to American core interests and values. To support the Army's cyberspace strategic goals to combat growing threats from other countries, the Army must focus and strive to produce world-class cyberspace professionals by investing substantial energies into innovative recruiting, talent management and retention endeavors.

15. SUBJECT TERMS
Cyberspace, Cybersecurity

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	40	

Putting the Pieces Together: Army Cyber Warrior Talent Management

(7,722 words)

Abstract

Cyberspace operations are critical to the success of the Department of Defense's (DoD) mission in a volatile, uncertain, complex and ambiguous multilateral world. Just as the United States envisions major armed conflict, cyberspace operations are an existential risk to American core interests and values. To support the Army's cyberspace strategic goals to combat growing threats from other countries, the Army must focus and strive to produce world-class cyberspace professionals by investing substantial energies into innovative recruiting, talent management and retention endeavors.

Putting the Pieces Together: Army Cyber Warrior Talent Management

> It's the great irony of our Information Age—the very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox—seen and unseen—is something that we experience every day.
>
> —President Barack Obama[1]

Over the past decade, the importance of cyberspace operations as a part of the United States and international military capabilities grew exponentially. Today, the volume and sophistication of cyber and physical attacks continue to rise.[2] In the United States alone more than one hundred foreign intelligence agencies continually attempt to infiltrate Department of Defense (DoD) networks.[3] More importantly, the emergence of the newest warfighting domain, cyberspace, has resulted in monumental changes in the U.S. Army's mission, focus, and structure.

United States' vulnerabilities steadily increase to the complexities of cyberspace because of how they uniquely affect all aspects of human interaction. The first line of defense required to protect against modern day cyberattacks is highly skilled cybersecurity talent. Unsurprisingly, facilitating the discovery and maturing of the cybersecurity genius is not just a significant challenge for the military or the United States. The pipeline for cybersecurity professionals is limited in both private industry and globally, too. However, because of the wide range of technical skills and abilities required, the process of growing the pipeline will take several years. Meanwhile, federal government agencies' partnerships with the larger cybersecurity community (private sector and academia institutions) provide a huge boost to the national security posture. The foundational efforts made thus far is likely to steadily accelerate and provide substantial growth in the cybersecurity talent pipeline.

The more relevant dimension the Army must focus on is an organizational cultural change to build and sustain the progress made to date. The caliber of the workforce to underpin the United States' and Army's efforts to elevate as a global leader in the cyberspace domain does not fit the mold of the traditional Soldier or civilian. To build on the Army's efforts already implemented, the organizational culture transformation needed requires a strategy and operational approach committed to a renewal in thought, eliminating or minimizing parochial politics and a paralyzing bureaucracy. The transformation is a paradigm shift in particularly the Army' personnel management system for critical, specialty Soldiers and civilians.

Senior leaders must lead the efforts in changing the culture and anchor these adjustments in the institution's social norms and values without compromising the seven fundamental Army values. Most importantly, revamping the Army's human resources recruitment and management for the cybersecurity workforce does not require leaders to travel in unchartered territory. There are reputable private sector companies excelling at recruiting, managing, and retaining their most essential commodity—the workforce. Google is one of the most lauded modern day companies that dominates the challenges of human resources operations. Ironically, many may likely argue that the Army can never implement a strategy similar to Google because Google's strategy does not correlate with Army's culture. Over the past few years, Army leadership made the initial steps to remove the roadblocks, looked beyond the existing boundaries (e.g. laws, regulations), and embarked on a relentless pursuit to dominate the cyberspace domain. The federal government and Army leadership must open the aperture of their critical thinking and allocate the appropriate resourcing. Moreover, the Army must still inculcate

real cultural change from the top to bottom. Real cultural change creates a lasting evolutionary imprint of change on the Army as a professional institution that is capable of recruiting, managing, and retaining Army cyber warriors.

The strategy to implement the desired changes is not an easy endeavor. An environment of limited resources, stiff competition, and growing demands further exacerbates the creation of innovative solutions required to set the stage for dominating the cyberspace domain. This paper highlights the evolution of DoD's cyber strategy and examines the Army's current initiatives to address the significant cyber talent management challenges. This paper also provides recommendations on how best to accelerate closing of the gap in recruiting, managing, and retaining a highly skilled cybersecurity workforce.

The Cyber Landscape

On the modern battlefield, securing cyberspace is a leading priority for any military in the 21st century. The days of the natural domains—land, sea, air, and space—being the only dimensions considered in the planning and conduct of operations have passed.[4] The newest warfighting domain, cyberspace, demands unprecedented degrees of collaboration and intersects all of the four traditional warfighting domains. The former Commanding General of Army Cyber Command (ARCYBER), Lieutenant General Edward Cardon, asserts, "Army commanders must fully embrace cyberspace as a new maneuver domain to maintain our freedom of action."[5]

"In response to the proliferation of cyber threats, the White House [recently] raised the U.S. DoD FY2016 cyber budget to $9.5 billion, an 11 percent increase in spending over FY2015."[6] The White House reserved $500 million of the FY2016 DoD cyber budget for the training and support of the Cyber Mission Forces (CMF).[7]

> The recently published DoD Cyber Strategy seeks to strengthen the U.S.' cyber defense and deterrence posture by building cyber capabilities and organizations around three critical cyber missions: the defense of DoD networks, systems, and information; the defense of the U.S. and its interests against cyberattacks of significant consequence; and the provision of cyber capabilities to support military operations and contingency plans.[8]

This integration of our nation's cyberspace operations for the combatant commanders required the standup of a Joint Force Headquarters-Cyber by each of the U.S. Cyber Command (USCYBERCOM) Service cyber components—ARCYBER, Fleet Cyber Command (FLTCYBER), Marine Corps Cyberspace Command (MARFORCYBER), and Air Force Cyber Command (AFCYBER). USCYBERCOM mandated each Service component provide an array of cyber forces and capabilities to defend DoD Information Networks (DoDIN), bolster the capabilities of combatant commands, and strengthen our nation's ability to withstand and respond to cyberattacks of significant consequence. The Army is the largest service contributor to the DoD's CMF with 41 teams of cyber Soldiers and civilians.[9] The Total Army Cyber Force also consists of an additional 21 Army Reserve and National Guard cyber teams.[10] The addition of the Army Reserve and National Guard is a critical component of Army's cyber workforce. In most cases, reserve component cyber experts are a tremendous resource because these Soldiers already have the acquired skills by way of private sector employment. Training from scratch is not required making integration much easier. The inclusion of the reserve component also provides a viable option to retain transitioning active duty service members into the private sector.

A national operational cyber strategy and appropriated funding alone are not sufficient to achieve dominance in the cyberspace operational environment. Furthermore, cyberspace technological dominance is unachievable without a skilled

workforce capable of operating at the highest level of the cybersecurity field. In Cybersecurity and Cyberwar, strategist Peter Singer asserts, “we [the United States] often frame cybersecurity as a technology problem. [Instead] it is a human problem.”[11] Hence, building capacity for our cyber professional workforce warrants a sense of urgency and first priority. In the Cyber Strategy, our nation’s senior political and military leaders acknowledge that the building of the CMF as DoD’s first strategic cyber goal is paramount for the United States to achieve global cyber dominance.[12]

However, the limited pipeline of qualified cyberspace candidates in the United States creates complex challenges in the Army’s long-term roadmap to recruit world-class cyberspace professionals. For example, “one RAND Corporation study estimates there are around 1,000 top-level cybersecurity experts globally versus a need for 10,000 to 30,000.”[13] Cybersecurity professionals are much like our linguists or special operations forces personnel. The candidates need highly specialized skills that require extensive training. Therefore, to secure the information that fuels both our national defense and our economic prosperity effectively, the Army must invest in a substantial long-term commitment to ensure that the Army has a highly trained and qualified cyber workforce at the ready.[14] “The cyber workforce is our nation’s most valuable asset today and must remain a national priority in the years ahead if the United States expects to achieve cyberspace domain superiority.”[15] An added complexity to the Army’s talent management system’s initiative lies in the fact that the Army is not only in competition with the other armed services but also other civilian agencies and the private sector.

Army’s senior leadership understands that people are our institution’s most valuable assets—our secret weapon to successfully achieve our strategic goals. The

strategy to obtain these highly valued assets relies heavily on the Army's talent management skills. In 2015, the Mission Command Center of Excellence published a White Paper on *Talent Management in the Army*, which defines talent management as "the systematic planning for the right number and type of people to meet the Army's needs at all levels and at all times so that the majority of them are employed optimally."[16] Hence, the Army must "integrate accessions, retention, development, and employment strategies."[17]

The talent management challenge to build the desired cyberspace workforce is a moving target. Within DoD, the cyberspace workforce requirements will likely continue to grow exponentially as well as cyberspace's capacity. Cyberspace touches virtually every individual aspect of our lives and the further digitization of all facets of the Army's work environment is inevitable. In light of the significant vulnerabilities cyberspace injects into our daily lives, the Army needs to address service specific cyber workforce challenges and aggressively commit to taking the initial steps necessary to close the gap.

One of the first steps in building a professional cybersecurity workforce entails recruiting manpower that possesses the niche capabilities to operate in the cyberspace domain. Several reports from organizations such as Booz Allen Hamilton and the Center for Strategic International Studies argue that the shortage of cyberspace manpower is not merely a global issue, but is the worst for the federal government in the United States.[18] Moreover, universities and colleges are not fully contributing to the cybersecurity talent pool, by way of, academic institutions not graduating students with profound technical talent and the security basics required to confront the wide array of

cyber threats on the modern battlespace.[19] However, in the last few years, universities have risen to the challenge with significant growth in the implementation of cybersecurity educational programs.[20]

The Army as an institution also faces challenges in eliminating gaps in the newly established training curriculum for all three phases of building the cybersecurity workforce. The efforts to integrate cybersecurity components into our existing training curricula are commendable thus far. However, over the past couple of years, relevant training issues exist in onboarding the initial cybersecurity professionals into the Army's ranks. The training pipeline at Army specific schoolhouses, specifically the Cyber Center of Excellence (CoE) located at Fort Gordon, GA, has a limited capacity. The course allocations are small. In fact, so small that the Army cannot allocate an adequate number of seats for the reserve component Soldiers.[21] As the Army continues to grow the cybersecurity force, the requirements for realistic cyber training environments rise, too. In fact, cyber persistent training environments exist for active and reserve components in limited areas within the United States, but the capacity does not meet the current Army training requirements.[22] In 2016, DoD designated the Army as the Executive Agent for DoD cyber ranges to better keep pace with each respective armed services' and the joint community's realistic training requirements.[23]

As the Army reorients educational objectives for grooming the newly acquired cybersecurity workforce, many may consider cyberspace operations as merely a specialized, highly technical field. Yes, formal technical education may better prepare a candidate to perform effectively in a cyberspace environment; but the Army needs to be careful not to unknowingly create barriers or limit the scope of the talent pool. The

possibilities of finding suitable candidates outside of Science, Technology, Engineering and Mathematics (STEM) or cyberspace educational backgrounds and professions are highly probable. Hence, the Army must utilize a high quality assessment tool to identify these highly sought out professionals. The Army's current accession tool, the Armed Services Vocational Aptitude Battery (ASVAB) test, is not sufficient without augmentation.[24] The test does not measure the aptitude for the responsibilities assigned to the Army by the DoD, defensive and offensive cyberspace operations.

In addition to the challenges of high competition and relevant onboarding assessments, a Booz Allen Hamilton study concluded that the federal government civilian hiring process is broken.[25] Many of the survey respondents quantified the process as inflexible, onerous, time-consuming and slow.[26] The subpar badging and credentialing program contributes significantly to the creation of this inefficient, lengthy hiring process.[27] The credentialing program also creates additional barriers in the Army's competition with the private sector for qualified cybersecurity candidates. Civilian personnel often must wait months at their commands to start work due to long wait times to obtain approval of initial or existing security clearances.[28] Recruiting these civilian cyberspace experts is just as vital to the Army's success as the military cyber workforce component. Civilian cybersecurity professionals account for 30 percent of the Army's cyber workforce.[29] Notably, unlike the Service's military counterpart, the Army has zero recruiters on hand to focus on hiring qualified civilian candidates. Between 16,000 and 20,000 civilian hires, join the ranks of the Army's talent pool each year.[30]

Another challenge the Army must address is the inability to compete with the private sector's incentive structures.[31] If the Army does not take action to lobby with the

U.S. Executive and Legislative branches to relook authorities for the recruitment and retainment of cybersecurity professionals, closing the talent pool gap remains a complex challenge. The Army cannot compete with the higher salaries, especially those associated with the top one to five percent of the overall national cybersecurity workforce, with its existing pay table and allowances.[32] Instead, the Army must better understand the 21st century cybersecurity workforce's values and priorities. The creation of valued tangible and intangible incentives are generally highly desirable to any workforce and likely remains an effective recruitment and retainment tool in today's society.

Even if the Army overcomes these and other challenges, the Army still operates in the age of government spending restrictions, better known as sequestration, to reduce our national debt. Any strategy to close the gap and build the cybersecurity workforce requires a sustainable resource (funding) strategy. Most recently evidenced by President Barack Obama's FY2017 budget proposal, cybersecurity is a top priority for each armed service and other federal agencies. The proposal sought $19 billion for cybersecurity across the federal government, a surge of $5 billion over the year.[33] While expectations are that cyber continues to gain additional appropriated funds, Army senior decision makers must ensure they effectively assess their decision space and take the appropriate risks. More importantly, they must remain vigilant in the responsible allocation and expenditure of monetary resources to appropriately resource the Army's plan.

The Army is in the initial stages of closing the cybersecurity professional talent gap. The blueprint required to address the critical personnel shortages will not be a

quick fix. Instead, the effort will likely take the Army several years to see marked improvements. There are several current initiatives already implemented by the Army to create a world-class cybersecurity workforce. “Army has established the Talent Management Task Force (TMTF) to integrate and synchronize Army efforts to acquire, develop, employ and retain a high quality force that can fight and win against any adversary in the world on the battlefield.”[34] The strategy map created by TMTF lays out the ends, ways, and means to optimize the talents of all Army Professionals.[35] More importantly, “[TMTF aims to] enhance Army readiness by aligning individual capability with the Army’s needs while optimizing human performance and engagement.”[36]

“[Today], the Army is the only service that has launched a dedicated cyber career field to manage Soldiers throughout their careers.”[37] In September 2014, the Army created the first new Army career branch in nearly 30 years—the Cyber Branch and Career Management Field.[38] Each year the Cyber CoE at Fort Gordon is responsible for educating these cyber Soldiers in one of the Army’s most academically rigorous training programs.[39] In-service recruiting of Soldiers with cyber-related jobs in the Signal and Military Intelligence Corps provides a constant inflow of Soldiers into the Army Cyber Branch.[40] “Today we have 397 officers, 141 warrant officers, and 560 non-commissioned officers and Soldiers in the Army’s recently created cyber branch.”[41] While 30 new cyber lieutenants graduated this year and will ramp up to 45 next year from West Point and the Reserve Officers’ Training Corps (ROTC).[42] Now, how does the Army continue to build and maintain the pipeline for these new cybersecurity professionals?

ARCYBER has three priorities mandated by USCYBERCOM. The third priority is to organize, man, train and equip ready cyber forces.[43] In efforts to enhance Army's cyber readiness, ARCYBER collaborates with DoD and private industry. The service component command currently partners with DoD's Hacking4 Defense program at Stanford University in California.[44] In partnership with private industry to promote cybersecurity, ARCYBER also initiated the Silicon Valley Innovation Pilot.[45] The pilot's objective is to find ways to counteract the use of social media and malicious actors.[46] Unexpectedly, the pilot's efforts have led to the successful employment of tools in our fight against the Islamic State of Iraq and the Levant (ISIL).[47]

The United States Military Academy (USMA) at West Point also has a vital role in ensuring the Army can establish a more competitive and security advantage in the cyberspace domain. A major discipline does not exist yet; but cadets can select a minor in courses such as Cyber Security Engineering and Cyber Operations, among others.[48] The Cyber Research Center (CRC), housed in the USMA Department of Electrical Engineering and Computer Science, spearheads extracurricular activities to enhance the cadet's cybersecurity exposure.[49] "The CRC provides educational opportunities to cadets in the areas of information assurance, information warfare, and forensics," in addition to, organizing and hosting annually the Cyber Defense Competition, cadet trip sections, annual summer internships and cadet mentorships.[50] The newly established cybersecurity curricula and CRC's latest initiatives also greatly attributed to the academy's capacity to create a highly competitive young, college-aged cybersecurity team. The USMA Cadet Competitive Cyber Team (C3T) is a globally ranked Capture

the Flag (hacking) team that participates in undergraduate and professional cybersecurity competitions hosted around the world year-round.[51]

The Army's bridge builder and cyber innovation agent, the Army Cyber Institute (ACI), is located at West Point, too.[52] "ACI is responsible for developing partnerships between the Army, academia, government, and industry while providing insight into future cyber challenges through interdisciplinary analysis on strategic cyber initiatives and programs."[53] In light of ACI's cyber innovation agent responsibilities, the Cyber Leader Development Program (CLDP) is an initiative created and operated by ACI.[54] The program provides an additional 800+ hours of impactful experiences through one-on-one mentorship, internships, conferences, clubs and seminars to USMA cadets outside the classroom.[55] CLDP offers the same opportunities to ROTC cadets, too.[56]

Since the cybersecurity workforce shortfall is a national problem shared with other armed services, federal government agencies, and private industry, the Army stepped up its efforts to improve collaboration with all stakeholders in the United States cybersecurity community. The most current joint initiatives include:

- *DoD's Scholarship for Service (SFS) programs.* DoD established SFS to counter "1) impending retirement of DoD's STEM workforce; 2) low college readiness rate and interest in STEM majors; and 3) challenges that the DoD, like other Federal employers, face in recruiting and retaining high-quality STEM talent in a competitive environment."[57] This program provides scholarships that may fully fund the typical costs incurred by full-time students while attending a participating 4-year institution, including tuition, education, and related fees.[58] Additionally, participants receive stipends of $22,500 for

undergraduate students and $34,000 for graduate students.[59] The National Science Foundation awards and funds these scholarships through grants.[60] SFS generates 120 graduates a year.[61]

- *Advanced Course in Engineering on Cyber Security (ACE-CS).* ACE-CS, modeled after the 80-year old General Electric Advanced Course in Engineering, is a public-private partnership to develop top ROTC cadets into next generation cyber leaders.[62] The program provides the cadets exposure to 1) an intense classroom environment with real-world problems; 2) professional cybersecurity mentorship, and 3) internships.[63]
- *Pathways Internship Program.* Presidential Executive Order 13562, dated December 27, 2010, refined the ground rules for service authorities to clear paths to internships and potential civil service careers for students and recent graduates.[64] Pathways affords students from high school to graduate level the opportunity to work in agencies and explore Federal careers while still in school and being paid for the work performed.[65]
- *Cyber Aptitude Test.* The ASVAB does not have the parameters to identify cybersecurity talent. In collaboration with the United States Air Force, the Army is actively engaged in a pilot to develop an assessment tool to measure a candidate's aptitude for defensive and offensive cyber operations.[66]
- *National Stakeholder Collaborative Events.* In hopes of strengthening the Nation's cybersecurity posture, Army hosted multiple industry events including a Joint Service Academy Cyber Summit with industry

executives.[67] Semi-annually Army also hosts a Cyber Talks event at the National Defense University that convenes cyber innovators from industry and inside the DoD to share ideas.[68]

Collaboration alone does not adequately grow the cybersecurity pipeline. Increasing the pipeline prompted the Army to implement organizational policy and structure adjustments to prepare the pipeline. DoD is currently engaged in an effort to create a new personnel system for the civilian cyber force. Much like the Army's new military Cyber Branch, the new personnel system provides DoD entities a more direct and consolidated management structure to hire, fire and pay civilian employees in critical cybersecurity posts.[69] DoD cyber specialists' salaries are forecasted to reach as high as $132,000 a year.[70] This new system bypasses traditional hiring rules and implements a new recruiting process.[71] A new Cyber Workforce Management Board oversees and governs the civilian personnel system.[72] The DoD Chief Information Officer, the undersecretary of Defense for personnel and readiness, and the department's principal cyber adviser jointly chair the board.[73] Additionally, all military services have a seat on the board.[74]

In a very short time, the Army gained approval for the implementation of tangible incentives for military and civilian personnel performing duties in CMF positions. Presently, the Army has implemented special duty assignment pay, assignment incentive pay, and bonuses for Soldiers serving in operational cyber assignments.[75] Table 1 below depicts the new incentives.

Table 1. Army Cyber Force Incentives[76]

Note: Cyber Mission Force (CMF) special pay up to $500 a month for accession and retention incentives.

Type	Requirements	Certification	Amount
Assignment Incentive Pay (AIP)	1) cyber speciality MOS 2) Good standing 3) 1-3 year CMF assignment	Apprentices Journeymen Masters	$200/month $300/month $500/month
Special Duty Assignment Pay	1) CMF position 2) Enlisted, PFC and above 3) Demanding position, requiring high degree of training and responsibility	Apprentices Journeymen Masters	$200/month $300/month $500/month

The Army has also expanded cyber educational programs, to include training in industry, fellowships, civilian graduate educations, and utilization of inter-service education programs (e.g. Air Force Institute of Technology, Naval Post Graduate School).[77] In the Guard and Reserve components, retention bonuses exist for active force Soldiers transitioning into cyber, in addition to, future accession bonuses for commissioned and warrant officers going into Reserve-component cyber.[78]

Several initiatives exist for the civilian workforce to recruit and retain qualified Army civilian cybersecurity professionals in the ranks alongside the military component. In the past two years, DoD and the armed services successfully implemented:

- Expedited hiring authority (direct-hire),
- Information Assurance Scholarship Program (IASP) funding increase for recruitment and retention,
- Cyber workforce loan repayment program,
- Information Technology (IT) Special Salary Rates restoral,
- IT and Cybersecurity certification bonuses, and
- Increased educational opportunities (e.g. NDU iCollege).[79]

The Army's current initiatives are commendable efforts. The accomplishments thus far took a collaborative effort by senior leaders external and internal to the Army.

Despite the promising outlook promoted by today's initiatives, there is still more strategic work to be done to build a world-class cybersecurity professional workforce to keep pace with our competitors and achieve global dominance in the cyberspace domain. To resolve this complex problem, perhaps the Army must seize the initiative and research the talent management models of reputable companies competing in the cybersecurity community.

A Different Perspective: An Industry Model Approach

Google is one of the top cited examples of corporate culture. In 2016, Fortune magazine hailed Google as the number one world employer for the seventh time in ten years.[80] A key ingredient to Google's success in a highly competitive digital environment is a belief that continuous innovation requires a new kind of people management.[81] More importantly, the best-laid plan or strategy is no substitute for talent. According to Google's senior leadership, talent hiring is not just the most important thing they do; but "hiring is the most process-driven thing [they] do."[82] Therefore dedicated investments into the time and energies required to get the best, starting with great people management, recruits the right people for the right job.

The transformative conventions of Google's recruitment and retention strategies prompted Google to rename the human resources division to "People Operations."[83] People Operations is the core of the company.[84] The staff, as well as the rest of Google's employees, are actively engaged in searching for people that will fit into the Google culture. A culture that strives to recruit creative, principled, and hardworking stars. In order to find these stars, Google opted to embark on a new frontier for management and recruitment referred to as "human capital analytics.[85] Human capital

analytics is a non-traditional analytical and data-driven approach focused on predicting the best candidates capable of succeeding at any job position in question.[86]

The statistics and algorithms used ensures that People Operations does not focus on the usual suspects—eliminates the biases—but instead better understands Google's environment and identifies the "ideal" candidate.[87] For example, favoring specialization over intelligence is exactly wrong, especially in high-tech environments, which change so fast.[88] Whereas a very high IQ is important and often chosen, Google values the ability to learn and absorb information as a more important trait. Additionally, the cyberspace domain's potential future growth is exponential, not linear, which further justifies that the ideal candidate should be a "learning animal" that possesses a desire to keep learning when faced with challenges.[89] Psychologist Carol Dweck defines this state of mind as the "growth mindset" where one's abilities are not fixed.[90] Individuals favor learning goals and not performance goals thus not worrying so much about risks or having to adapt to constant change.[91]

The second type of ideal candidate penned by Google is the "smart creative." Most companies arguably focus on the premise knowledge is power. Well, Google takes knowledge as power a step further by recognizing that the technical expertise is a desired attribute but a multidimensional person capable of combining the technical depth of their trade with business savvy and creative flair are the key to achieving success in today's Internet Century.[92] These people are not knowledge workers in the traditional sense but *smart creatives*. In order to find the *learning animals* and *smart creatives*, Google recruits candidates from a wide variety of avenues and sources in

industry, to include employee referral, college recruitment, professional networking, recruiter trainers, ad-word search engines contests, and brain teasers.[93]

Google's successful, dynamic talent management strategy must stress not only recruitment but also the management and retention of these highly sought after talented professionals. In light of the limited pipeline of individuals in the career fields Google desires, the focus on understanding what motivates people and how to engage people individually is critical to Google meeting its People Operations' objectives. Figure 1 below depicts the employee proposition Google relies upon to achieve a genuine understanding of their talent pool and individual's motivations.

Employee Proposition = environment + work + growth + reward + flexibility

Figure 1. Google Employee Proposition[94]

Generally, people spend most of their time every day in their respective work environments. Therefore, a pleasant, engaging atmosphere is vital as well as providing individuals an environment to look forward to coming to each day. Google's reliance on the "herd effect" has greatly attributed to the company's success in people management. Google defines *herd effect* as "a workforce of great people [that] not only does great work; the *herd effect* attracts more great people."[95] The best workers tend to follow each other because the best workers want to seize the opportunity to work alongside one another to share their ideas. The great work and innovation facilitated by this enhanced collaboration nurture more creativity and employee efficiency.[96] Surprisingly, some of the most effective Google rewards regarding *smart creative*

retention does not focus on monetary reward but fostering a team spirit and a sense of community.[97]

Innovators and top performers gravitate to Google environments where firms take bold actions, take major risks and provide innovators with freedom and resources to innovate.[98] Google understands work must provide job satisfaction to their community as a group and individual. The company is exceptional at providing job enrichment by way of ensuring their workers take on several projects and accept full ownership of all of their projects from beginning to end.[99] Conducting operations in this manner give each worker a sense of ownership and a great feel for how the individual affects the company's operations.

Another important aspect of the workplace to the workforce is learning and development opportunities. Google advertises itself as a learning organization. With the use of analytics and statistics, Google assigns a mentor to everyone with whom they can confidentially discuss career development plans and any other areas of concerns.[100] At Google, opinions do matter. The promotion of their town hall events, weekly all-hands sessions, and their Google-o-Meter provides all of their staff members an opportunity to engage with senior staff management about work-related questions.[101] The Google-o-Meter is a repository of staff recommended policy or perks that everyone votes on to gauge whether or not implementation would be a means to foster a better work environment.[102]

Most times companies aligned with the highly technical industries, attribute successful human resources operations and a healthy work environment to money. Google's People Operations does not singularly focus on money as a factor to attract

the desired *smart creatives*.[103] Google has an outstanding benefits package and service incentives.[104] The company's senior management has witnessed firsthand that people seldom leave over compensation, especially solely monetary objections.[105] Employees, more importantly, want their supervisors to hear and consider them a valued member of the team. They want to be able to accomplish great challenging things, work with great people, and work in an inspiring company culture.[106] In regards to pay and promotion, a group of peers, committee or a dedicated, independent team makes those decisions.[107]

The Google environment is an ideal workspace. At Google, employees experience a flexible, non-threatening environment to expand their horizons. Google gives employees freedom, a healthy work-life balance, incredible rewards and even the chance to have fun at work.[108] Many may believe Google's departure from the traditional human capital management is too radical. Yet this relatively young company continues to break barriers, attracting and leveraging the talents of true innovators.

"Google's exceptional success shows how far a company can go when leaders celebrate and nurture the staff, rather than considering them replaceable tools."[109] The company holds firm to the value-added proposition offered to each employee—environment, work, growth, reward, and flexibility. Google staffers experience daily great challenges, a great atmosphere, great rewards, great pride, and great communications, along with great bosses. The Army can take a page out of Google's book to traverse the wall that stands between the Army and the Service's capability of effectively defending our Nation in the globally contested cyberspace domain. Notably, Army Secretary Eric Fanning stated, "I think everybody can agree that we can't build and retain a cyber force like we have done traditionally with other aspects of the

force."[110] Cybersecurity experts are among the most sought after professionals in the technical sector by a wide margin. The Army must think beyond the existing traditional, prescribed process for recruitment, management, and retention of cybersecurity professionals to evolve and keep pace with proven best practices in the private sector.

Closing the Gap: Cybersecurity Workforce Management Framework

The Army is leading the way as far as the armed services in regards to the talent recruitment and management of society's highly sought after cybersecurity workforce.[111] Likely one of the most critical components in the Army accomplishing ARCYBER's resolute priorities to meet the demands of the cyberspace warfighting domain is—the PEOPLE. Yet despite the notable advancements made in the last couple of years, the Army still has challenges recruiting, managing and retaining cybersecurity professionals. Organizational culture adjustments—a leap from parochial norms—is necessary to close the gap. Think of the Army's cybersecurity workforce in the context of a balloon. A balloon in its original form is incomplete, useless. The balloon cannot perform its intended purpose until you breathe life into the balloon. In order to overcome some of the difficulties faced thus far, transformation—a new way of thinking—within the Army organization can cultivate endless possibilities for the future Army cybersecurity workforce. The Army does not have to recreate the wheel but learn and build from the experiences of private sector competitors such as Google to grow highly efficient, innovative teams. The Army must champion policy changes and initiatives that guarantee future Army cybersecurity professionals the ideal environment, work, growth, reward, and flexibility.

"Certainly new systems, policies, and procedures can force changes in behavior, but often what senior decision makers truly desire is a shift in attitudes—a culture

change across the entire Army."[112] As for successfully building a cyber workforce, there are still indicators that the Army's organizational culture is still slightly misaligned with the desired environment for the cybersecurity professional. Real organizational change in a mature organization requires not only a concerted effort from top-to-bottom leadership but also the application of effort and resources to key pressure points in the Army institution.[113] Edgar Schein, a notable author in the field of organizational development, equates these efforts and resources as embedding and reinforcing mechanisms.[114] The embedding and reinforcing mechanisms required to replicate Google's employee proposition and further advance the Army's efforts in building an elite cybersecurity workforce aligns with three lines of efforts. The three lines of efforts critical to best shape Army's way forward to build a professional cybersecurity force include: Acquiring, Maintaining and Retaining cybersecurity Soldiers and civilians.

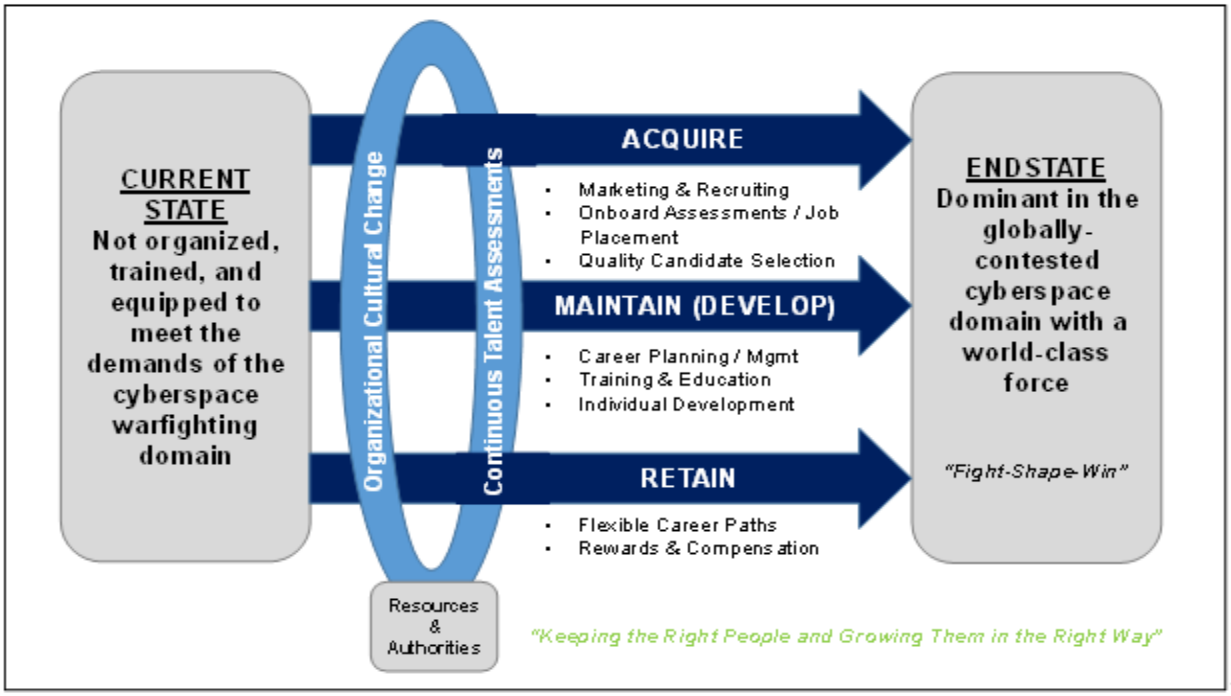


Figure 2. Cybersecurity Workforce Management Framework[115]

The Army must maintain an aggressive momentum in future marketing and recruiting strategies to compete with other armed services, government agencies, and the private sector effectively. Moreover, when addressing issues within the cybersecurity arena, all of the United States' federal and private stakeholders must continue to collaborate. The relationships and initiatives the Army currently uses as a collaborative platform with the academia community and industry are integral in the continued growth of the United States cybersecurity workforce pipeline now and in the future.

Onboarding and Job Placement Assessments

The next generation of technology leaders will be on the front lines protecting our national security and economic stability. Hence, Army leaders must not compromise the importance of Army values. Why? Actions in the cyberspace domain will more than likely have strategic implications. In addition to values, the Army understanding what motivates this cybersecurity generation as a whole is critical—regardless of an individual's educational background. If the Army knows what cognitive and aptitude measures to screen for, leaders can better codify the Army's requirements for both civilian and military professionals. The use of an analytical assessment tool similar to Google's non-traditional human capital analytical assessment tool and Google's data points can improve Army's ability to the select the right people (*smart creatives and learning* animals) for the right jobs.

Expanded Direct Commissions to the Cybersecurity Career Field

Direct commissions already exist in the Army's medical, judge advocate and chaplain corps for civilian-degreed leaders in the private sector. Expansion of this policy potentially alleviates Army's issue with recruiting the upper tier cybersecurity

professionals that possess the experience and skills capable of detecting advanced persistent threats. The special skills attributed to the upper tier cybersecurity professionals are critical to sustaining military operations in the 21st century. Direct commissions are a low-risk initiative that ensures the aperture of the talent pool is not de-scoped unintentionally.

Streamlined Security Clearance Process

Many cybersecurity positions, military and civilian, require some form of security clearance. The federal security clearance adjudication process complicates the recruiting process. The waiting period is a consistent grievance of individuals seeking cybersecurity positions not only in the Army but also across all entities in the federal government. The DoD in partnership with the rest of the cybersecurity community, federal and state, must invest energies in streamlining the process and procedures to obtain or revalidate security clearances. Most importantly, all entities must be more willing to share information and eliminate duplicative efforts. Time is of the essence. Cyberattacks occur every minute of every hour and there are numerous cybersecurity positions that remain unfilled.

Creation of Civilian Cyber Career Fields

The Army invested significantly in the design and implementation of the Cyber Branch and Career Management Field for the military. Whereas, a huge shortfall still exists in the government civilian sector. There is no specific occupational series to identify federal civilian cybersecurity positions. The current positions merely cover the basic, general Information Technology knowledge, skills and attributes. The occupational series are outdated and in need of immediate restructure to ensure, the right people or selected for the right jobs in the civilian sector who make up thirty

percent of the workforce. This initiative must be the highest priority for the newly formed DoD Cyber Workforce Management Board of which the Army is a participating board member.

Overhaul of the Up and Out Career Progression System

In order to foster an environment that adequately motivates the cybersecurity professional, the Army needs to reexamine promotion policies. Under the up and out promotion policy, the Army forces Soldiers passed over twice for promotion out of the military.[116] This way of thinking is counterproductive. If the Army does not separate retention from promotion, the Army continues to lose valuable people that possess a vast breadth of knowledge, wisdom, and experience. Today's Army expects Soldiers to keep climbing the ladder toward senior management and leadership positions.[117] Cybersecurity professionals, just as many people in society, do not necessarily desire management or leadership positions.[118] This does not mean these individuals have no desire to continue to be productive teammates, unselfishly contributing to our collective efforts and completing his or her assigned tasks. They get job satisfaction when led and provided the opportunity to do their designated jobs, which in some aspects requires indirect leadership skills. Allowing these individuals to move up and out of the military only frustrates the Army's cybersecurity pipeline. These actions cost the Army human capital and the loss of critical special skills that the organization cannot afford to lose in a highly competitive, resource-constrained environment. Additionally, assessment tests tailored to the critical skillset qualifications established in the Army's cybersecurity career progression model must manage this critical workforce more effectively. Supervisor, peer and subordinate performance assessments should also be an integral

part of this continuous talent assessment process to build and maintain a world-class cybersecurity workforce.

Broader Educational Initiatives to Emphasize and Improve Cyber-Related Competencies for the ROTC Community

USMA is already an established incubator for future cyberspace strategic leaders. The opportunity exists for ROTC cadets to partake in programs such as the Army Cyber Institute's (ACI) CLDP just as USMA cadets; but ROTC participation is low due in part to poor strategic communications of the vast opportunities available to ROTC cadets. Nevertheless, the ROTC cyber educational system structure as the system exists today does not produce the cybersecurity strategic leaders needed in our ranks now and in the future. Improvements require the Cadet Command leadership's increased engagement along with working more in tandem with USMA, ACI, and the Department of Homeland Security Centers of Academic Excellence's cybersecurity educational efforts in producing top-quality cyber officers. Furthermore, the expansion of the participant pool and resolution of the security clearance backlog in the ROTC's Cyber Operations Internship Program (RCIP) requires elevated leadership engagement with DoD officials. The program is a promising initiative; but the current pipeline is limited.

Improve Scholarship for Service (SFS) Reach and Strategic Communications

The Army injected immense efforts in the force during the implementation of the new Cyber branch and the new cyber curricula at Fort Gordon to grow the cybersecurity community. The Army leveraged existing joint schools, training with industry and academia as appropriate for educating both the military and civilian cybersecurity workforce. In an effort to maintain a formidable, highly trained workforce, the Army must

invest additional marketing resources to increase leader, Soldier and civilian awareness of the vast opportunities provided by SFS and the Information Assurance Scholarship Program. For those active members, military and civilian, that desire a career migration into the cybersecurity community, they generally are not aware of opportunities that already exist. As for the general population, over 145 higher educational institutions with Centers of Academic Excellence (CAE) exist throughout the nation.[119] DoD must only work to eliminate the uneven distribution of the CAE programs. The majority of these programs are associated with 4-year colleges and very few 2-year community colleges, likely eliminating the throughput of some potential cybersecurity candidates.[120]

Implement Realistic Physical Fitness Requirements

The Army recently launched a new accessions physical fitness test for new recruits. The Army designed the test to determine if the recruits can meet the demands of certain specialty jobs such as infantry and armor. The key skills and attributes required for cybersecurity military professionals are not physically demanding. Physical fitness is a priority for cybersecurity Soldiers, but the requirements should not necessarily be the standard physical fitness test currently administered to the general population. Their standard physical fitness test must be appropriately adjusted to fit the physical requirements attributable to their work environment which is rarely, if ever, on the tactical or operational front lines.

Good News Story— Compensation

Compensation is only one of many components of effective talent management. Leaders must also consider job satisfaction, leadership, training, and education. These other components are of utmost importance in the absence of competitive federal monetary benefits. With the assistance of Congress and DoD, the Army made

significant gains in monetary incentives for the cybersecurity workforce. The successful implementation of monetary incentive models is a well-proven initiative for recruiting, maintaining and retaining specialty skills critical to the Army mission such as—aviation, medical, special operations, and foreign language programs. As for non-monetary compensation, the opportunities are endless and more manageable in light of the Army's evolving culture, the emerging threats, and the labor market competition (e.g. health care package). Non-monetary compensation should include items such as duty location preference, continuing education, job status, job satisfaction, family benefits, and stability. Again, the Army's main focal point must be what matters to cybersecurity professionals outside of money.

- Integrity of the employers matter most
- Isn't just about the competitive pay and benefits—challenging high-impact work and training matters
- Engage with other experts—work with others whose talent and work they respect and can learn from
- Opportunities for growth and advancement

Figure 3. What Matters to Cybersecurity Professionals[121]

Expansion of the Career Intermission Pilot Program (CIP)

An expansion of CIP to the cybersecurity workforce places the importance of gaining valuable expertise and human networking links over the misnomer that a break in service should be a negative career move. Congress authorized the program in 2009 as a retention incentive for all the armed services, but most services opted not to implement the pilot program until recently. The Army implemented the pilot in 2015, and the program currently applies to both officer and enlisted Regular Army, Army Reserve, and Army National Guard. This program with adjustments (i.e. enrollment criteria and increased sabbatical pay) provides an acceptable platform to offer "on and off ramps" for both military and civilian to the Army's and individual's benefit. During these

sabbaticals, the Army affords the cybersecurity workforce the opportunity to collaborate and grow professionally within the private sector. Our nation cannot overcome what lies ahead in the cyberspace domain unless all stakeholders work in concert.

Funding

The cybersecurity human capital crisis is real and negatively affects our nation's ability to dominate the volatile cyberspace domain. As early as 2010, the Executive Branch and Congress deemed cyber-related activities as a major priority for the nation.[122] Therefore, in concert with each armed service, DoD supports and directs measured growth in cyber initiatives. In order to implement any policy changes or initiatives previously mentioned to grow the cybersecurity workforce, the Army requires a sustainable resourcing strategy. Army senior leaders must remain engaged in supporting and promoting new initiatives leveraging the annual Planning, Programming, Budgeting, Execution (PPBE) process and be prepared to take calculated risks to meet our objectives. Inaction is not acceptable for this cyberspace problem set.

Conclusion

The Army understands cyberspace is an existential threat to our existence. The man-made domain is an interesting problem space for our strategic leaders. Since the inception of ARCYBER in 2010, ARCYBER has placed "significant emphasis on achieving unity of command for all Army cyberspace operations and eliciting unity of effort from all Army stakeholders."[123] Many senior Army leaders, just as the former Commanding General of ARCYBER, Lieutenant General Edward Cardon, affirm that "technology, as significant as it is in the rapidly changing face of warfare, will not be the deciding factor in who will dominate in [the cyber] domain. It's the people."[124]

> Proactive change is the cornerstone of a learning organization and is the result of an identified glide path with a well-known, attainable [vision] and self-reflection used to gain advantage to new ways of thinking—promotion of continual growth starting at the individual soldier level.[125]

In order to effectively recruit, manage, and retain highly valued cybersecurity professionals, a cultural change—innovative thinking and a new approach—must be non-negotiable at all levels of Army leadership. In large organizations much like the Army, there exists a tendency toward institutional calcification despite the obsolescence of practices long after strategic, environmental or technological change.[126] The Army must break the cycle—words without actions do not inspire or promote change. If the Army commits fully to implementing change, those actions will make the organization more capable as individuals and as an Army in the cyberspace domain. The organizational changes will move the Army even closer to closing the gap and make the Army a cybersecurity employer of choice in a highly competitive community. Furthermore, the Army is not the only United States stakeholder in cyberspace. Private industry primarily owns and operates the cyberspace domain.[127] In order to improve the nation's cybersecurity posture, the Army must eliminate duplicitous efforts and work with the other armed services, industry, and academia to create a pipeline of cybersecurity professionals with the deep technical skills required for the United States to sustain a competitive edge. Engaged action is essential to put the pieces together now to get the right people in the right place, at the right time to defend our nation in a domain of infinite possibilities and ever-changing threats.

Endnotes

[1] Booz Allen Hamilton, *Readying the Next Generation Cyber Workforce: Acquiring, Developing, and Retaining Cyber Professionals* (Washington, DC: Booz Allen Hamilton, 2010), 1.

[2] Diane Ritchey, "Why the Security Talent Gap is the Next Big Crisis," *Security Magazine Online*, May 1, 2014, http://www.securitymagazine.com/articles/85451-why-the-security-talent-gap-is-the-next-big-crisis (accessed December 30, 2016).

[3] William Mathews, "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 (accessed January 4, 2017).

[4] Edward C. Cardon, "The Future of Army Maneuver-Dominance in the Land and Cyber Domains," *The Cyber Defense Review* 1, no. 1 (Spring 2016): 19-20, http://www.cyberdefensereview.org/wp-content/uploads/2015/01/CDR-SPRING2016.pdf (accessed January 19, 2017).

[5] Ibid.

[6] Francesca Spidalieri and Jennifer McArdle, "Transforming the Next Generation of Military Leaders into Cyber-Strategic Leaders: The Role of Cybersecurity Education in U.S. Service Academies," *The Cyber Defense Review Online* 1, no. 1 (Spring 2016): 141, http://www.potomacinstitute.org/images/CDR_Spidalieri-McArdle_p141-p163_041216.pdf (accessed December 30, 2016).

[7] Ibid., 143.

[8] Ibid., 141.

[9] U.S. Army Cyber Command, "The Army's Cyberspace Advantage," *Stand-To!*, blog entry posted December 20, 2016, https://www.army.mil/article/179967/stand_to_the_armys_cyberspace_advantage (accessed December 30, 2016).

[10] Ibid.

[11] Joel Dreyfuss, "The Cybersecurity Talent War You Don't Hear About," *CNBC Online*, May 13, 2015, http://www.cnbc.com/2015/05/12/the-cybersecurity-talent-war-you-dont-hear-about.html (accessed December 30, 2016).

[12] Spidalieri and McArdle, "Transforming the Next Generation of Military Leaders," 143.

[13] Dreyfuss, "The Cybersecurity Talent War You Don't Hear About."

[14] Booz Allen Hamilton, *Readying the Next Generation Cyber Workforce*, 2.

[15] Ibid.

[16] Mission Command Center of Excellence, *Talent Management in the Army: Review, Comment, and Recommendation on Talent Management Models* (Fort Leavenworth, KS: U.S. Department of the Army, Mission Command Center of Excellence, April 2015), 6.

[17] Ibid.

[18] Martin C. Libicki, David Senty, and Julia Pollak, *Hackers Wanted: An Examination of the Cybersecurity Labor Market* (Santa Monica, CA: RAND Corporation, 2014), 15.

[19] Ritchey, "Why the Security Talent Gap is the Next Big Crisis," 22.

[20] Libicki, Senty, and Pollak, *Hackers Wanted: An Examination of the Cybersecurity Labor Market*, 18.

[21] U.S. Army Cyber Command, "Summit Brings Senior Cyber Leaders Together to Share Total Army Opportunities, Solutions," January 5, 2016, linked from *The United States Army Home Page*, https://www.army.mil/article/160551/Summit_brings_senior_cyber_leaders_together_to_share_Total_Army_opportunities__solutions (accessed December 30, 2016).

[22] Edward C. Cardon, "Maturing Cyber Capabilities Critical to the Army Future," September 21, 2016, linked from *The United States Army Home Page*, https://www.army.mil/article/175465/maturing_cyber_capabilities_critical_to_army_future (accessed December 30, 2016).

[23] Ibid.

[24] Panayotis A. Yannakogeorgos and John P. Geis II, *The Human Side of Cyber Conflict: Organizing, Training and Equipping the Air Force Cyber Workforce* (Maxwell AFB, AL: Air University Press, 2016), 53.

[25] Booz Allen Hamilton, *Readying the Next Generation Cyber Workforce,* 12.

[26] Ibid.

[27] Libicki, Senty, and Pollak, *Hackers Wanted,* 57-58; Yannakogeorgos and Geis, *The Human Side of Cyber Conflict: Organizing, Training and Equipping the Air Force Cyber Workforce*, 57.

[28] William Matthews, "Military Battles to Man Its Developing Cyber Force," *GovTech Works,* https://www.govtechworks.com/military-battles-to-man-its-growing-cyber-force/ (accessed May 1, 2017).

[29] Christopher Cline, "Cyber Command Reaches Strategy Milestone," *Army*, March 2015, 43.

[30] Jared Serbu, "DoD Debuting New Personnel System for Civilian Cyber Workforce," *Federal News Radio,* July 15, 2016, http://federalnewsradio.com/defense/2016/07/dod-debuting-new-personnel-system-civilian-cyber-workforce (accessed December 30, 2016).

[31] Jeff Akin, Roseann Ryba, and Eric Vazquez, *Acquiring the Right Talent for the Cyber Age: The Need for a Candidate Development Plan* (Washington, DC: Booz Allen Hamilton Inc., May 13, 2011), 1.

[32] Libicki, Senty, and Pollak, *Hackers Wanted,* 16-17.

[33] Reuters, "Obama Budget Proposal Includes $19 Billion for Cybersecurity," *Fortune,* February 9, 2016, http://fortune.com/2016/02/09/obama-budget-cybersecurity (accessed January 4, 2017).

[34] Army G-1, "Army Talent Management Task Force," *Stand-To!* blog entry posted August 11, 2016, https://www.army.mil/standto/2016-08-11 (accessed December 30, 2016).

[35] Ibid.

[36] Ibid.

[37] U.S. Army Cyber Command, "The Army's Cyberspace Advantage."

[38] U.S. Cyber Command Combined Action Group, "Beyond the Build: How the Component Commands Support the U.S. Cyber Command Vision," *Joint Force Quarterly Online* 80 (1st Quarter 2016): 92, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_86-93_CyberCom.pdf (accessed December 30, 2016).

[39] U.S. Army Cyber Command, "The Army's Cyberspace Advantage."

[40] Matthews, "Military Battles to Man Its Developing Cyber Force."

[41] Sydney J. Freedberg Jr., "U.S. Army Races to Build New Cyber Corps," *Breaking Defense*, November 8, 2016, http://breakingdefense.com/2016/11/us-army-races-to-build-new-cyber-corps (accessed December 30, 2016).

[42] Ibid.

[43] U.S. Cyber Command Combined Action Group, "Beyond the Build: How the Component Command Support the U.S. Cyber Command Vision," 87.

[44] Cardon, "Maturing Cyber Capabilities Critical to Army Future."

[45] Ibid.

[46] Ibid.

[47] Ibid.

[48] Spidalieri and McArdle, "Transforming the Next Generation of Military Leaders," 153.

[49] Ibid.

[50] Ibid.

[51] Ibid., 153-154.

[52] U.S. Cyber Command Combined Action Group, "Beyond the Build: How the Component Commands Support the U.S. Cyber Command Vision," 89.

[53] Ibid.

[54] Spidalieri and McArdle, "Transforming the Next Generation of Military Leaders," 154.

[55] Ibid.

[56] Andrew Schoka, "Training Future Cyber Officers: An Analysis of the U.S. Army ROTC's Efforts to Produce Quality Junior Cyber Officers," *Small Wars Journal*, September 10, 2016, 4, http://smallwarsjournal.com/jrnl/art/training-future-cyber-officers-an-analysis-of-the-us-army-rotc%E2%80%99s-efforts-to-produce-quality (accessed December 2, 2016).

[57] U.S. Office of Management and Budget, *National Defense Education Program RDTE Budget Item Justification, PB 2016 Office of the Secretary of Defense* (Washington, DC: U.S. Government Printing Office, 2015), 1.

[58] Ibid.

[59] *U.S. Office of Personnel Management Scholarship for Service Home Page*, https://www.sfs.opm.gov/ (accessed December 31, 2016).

[60] Ibid.

[61] Libicki, Senty, and Pollak, *Hackers Wanted,* 63.

[62] Kamal Jabbour and Susan Older, *The Advanced Course in Engineering on Cyber Security: A Learning Community for Developing Cyber-Security Leaders* (Syracuse, NY: Syracuse University, 2014), 1.

[63] Ibid., 2.

[64] U.S. Office of Personnel Management, "FAQs – Pathways Internship Program," linked from *U.S. Office of Personnel Management Home Page* at "Policy, Hiring Information, Students & Recent Graduates," https://www.opm.gov/policy-data-oversight/hiring-information/students-recent-graduates/ (accessed December 30, 2016).

[65] Ibid.

[66] Yannakogeorgos and Geis, *The Human Side of Cyber Conflict: Organizing, Training and Equipping the Air Force Cyber Workforce*, 54.

[67] U.S. Cyber Command Combined Action Group, "Beyond the Build: How the Component Commands Support the U.S. Cyber Command Vision," 89.

[68] Ibid.

[69] Serbu, "DoD Building a New Personnel System for Civilian Cyber Force."

[70] Matthews, "Military Battles to Man Its Developing Cyber Force."

[71] Serbu, "DoD Building a New Personnel System for Civilian Cyber Force."

[72] Ibid.

[73] Ibid.

[74] Ibid.

[75] Vergun, "Cyber Chief: Army Cyber Force Growing 'Exponentially'," *Federal Information & News,* March 5, 2015, in ProQuest (accessed December 2, 2016).

[76] Jim Tice, "Assignment, Special Duty Pays OKd for Cyber Soldiers," *Argus Leader,* April 21, 2015, http://www.argusleader.com/story/military/benefits/pay/2015/04/21/accession-retention-incentives-sdap/26119091 (accessed December 30, 2016).

[77] Vergun, "Cyber Chief: Army Cyber Force Growing 'Exponentially'."

[78] David Vergun, "Army May Create Cyber Career Field for Civilians," *Military.com*, April 17, 2015, http://www.military.com/daily-news/2015/04/17/army-may-create-cyber-career-field-for-civilians.html (accessed December 2, 2016).

[79] Libicki, Senty, and Pollak, *Hackers Wanted: An Examination of the Cybersecurity Labor Market*, 74-75; U.S. Office of Personnel Management*, Cyber Security Hiring, Pay and Leave Flexibilities* (Washington, DC: U.S. Office of Personnel Management, November 23, 2015).

[80] "100 Best Companies To For," *Fortune*, September 19, 2016, http://fortune.com/best-companies/google-alphabet-1/?iid=sr-link2 (accessed January 2, 2017).

[81] John Sullivan, "How Google Became the #3 Most Valuable Firm by Using People Analytics to Reinvent HR," *ERE Media Online*, February 25, 2013, https://www.eremedia.com/ere/how-google-became-the-3-most-valuable-firm-by-using-people-analytics-to-reinvent-hr (accessed January 2, 2017).

[82] Eric Schmidt and Jonathan Rosenburg, *How Google Works* (New York: Grand Central Publishing, 2014), 95; Lisa Jackson, "The Real Secrets of Google's Corporate Culture," *Corporate Culture Pros*, blog entry posted July 23, 2013, https://www.corporateculturepros.com/the-real-secret-of-googles-corporate-culture/ (accessed October 4, 2016).

[83] Elizabeth Matsangou, "Secrets of Google's Talent Retention Success," June 15, 2015, http://www.europeanceo.com/business-and-management/secrets-of-googles-talent-retention-success (accessed January 2, 2017).

[84] Ibid.

[85] Ibid.

[86] Ibid.

[87] Schmidt and Rosenburg, *How Google Works*, 108-109.

[88] Ibid., 104.

[89] Ibid., 102.

[90] Ibid., 103.

[91] Ibid.

[92] Ibid., 17.

[93] "Talent Management Framework: Human Resources, Role, and Strategies at Google Inc," *Russia Robinson*, blog entry posted June 23, 2014, https://russiarobinson.wordpress.com/2014/06/23/talent-management-framework-human-resources-role-and-strategies-at-google-inc (accessed January 3, 2017).

[94] Matsangou, "Secrets of Google's Talent Retention Success."

[95] Schmidt and Rosenburg, *How Google Works*, 99.

[96] Matsangou, "Secrets of Google's Talent Retention Success."

[97] Ibid.

[98] Sullivan, "How Google Became the #3 Most Valuable Firm by Using People Analytics to Reinvent HR."

[99] Matsangou, "Secrets of Google's Talent Retention Success."

[100] Ibid.

[101] Ibid.

[102] Ibid.

[103] Schmidt and Rosenburg, *How Google Works*, 126.

[104] "Talent Management Framework: Human Resources, Role, and Strategies at Google Inc."

[105] Schmidt and Rosenburg, *How Google Works*, 126.

[106] Ibid.

[107] Matsangou, "Secrets of Google's Talent Retention Success."

[108] Ibid.

[109] Ibid.

[110] David Fastabend, Jeff Becker, and Greg Gardner, "Mad Scientist: The 2050 Cyber Army," *U.S. Army TRADOC G-2*, blog entry posted November 7, 2016, https://community.apan.org/wg/tradoc-g2/mad-scientist/b/weblog/archive/2016/12/06/mad-sci-army-cyber-2050-final-report (accessed December 30, 2016).

[111] Mathews, "Military Battles to Man Its Developing Cyber Force."

[112] Leonard Wong, *Op-Ed: Changing the Army's Culture of Cultural Change* (Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute May 16, 2014), 1.

[113] Stephen J. Gerras, Leonard Wong, and Charles Allen, *Organizational Culture: Applying a Hybrid Model to the U.S. Army* (Carlisle Barracks, PA, U.S. Army War College, November 2008), 17.

[114] Ibid.

[115] U.S. Department of the Army, *U.S. Army Talent Management Strategy: Force 2025 and Beyond* (Washington, DC: U.S. Department of the Army, September 20, 2016), 9.

[116] Carl Forsling, "The Up-or-Out Promotion System Hurts the Military," *Task & Purpose*, http://taskandpurpose.com/military-needs-abandon-promotion-boards (accessed January 4, 2017).

[117] Ibid.

[118] Franklin S. Reeder and Katrina Timlin, *Recruiting and Retaining Cybersecurity Ninjas* (Washington, DC: Center for Strategic and International Studies, October 19, 2016), 1.

[119] David J. Kay and Terry J. Pudas, *Preparing the Pipeline: The U.S. Cyber Workforce for the Future* (Washington, DC: National Defense University, August 1, 2012), 8.

[120] Ibid.

[121] Kenneth Corbin, "Cybersecurity Pros in High Demand, Highly Paid and Highly Selective," *CIO*, http://www.cio.com/article/2383451/careers-staffing/cybersecurity-pros-in-high-demand--highly-paid-and-highly-selective.html (accessed December 30, 2016).

[122] Kay and Pudas, *Preparing the Pipeline: The U.S. Cyber Workforce for the Future*, 2.

[123] Cardon, "Maturing Cyber Capabilities Critical to Army Future."

[124] Rodney D. Harris, "Army Braces for a Culture Clash," *Signal Magazine Online,* January 1, 2016, http://www.afcea.org/content/?q=Article-army-braces-culture-clash (accessed December 30, 2016).

[125] Thomas E. Meyer, "The Leadership Imperative: A Case Study in Mission Command," *Infantry Online*, January – March 2014, http://www.benning.army.mil/infantry/magazine/issues/2014/Jan-Mar/Meyer.html (accessed December 30, 2014).

[126] Mission Command Center of Excellence, *Talent Management in the Army: Review, Comment, and Recommendation on Talent Management Models*, 7.

[127] U.S. Cyber Command Combined Action Group, "Beyond the Build: How the Component Commands Support the U.S. Cyber Command Vision," 89.