2017-09

Recruiting the cyber leader: an evaluation of the human resource model used for recruiting the Armys "Cyber Operations Officer"

Nicholson, Wallace C.; Gibbs, Sean A.

Monterey, California: Naval Postgraduate School

http://hdl.handle.net/10945/56161

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

RECRUITING THE CYBER LEADER: AN EVALUATION OF THE HUMAN RESOURCE MODEL USED FOR RECRUITING THE ARMY'S "CYBER OPERATIONS OFFICER"

by

Wallace C. Nicholson
Sean A. Gibbs

September 2017

Thesis Co-Advisors:	Steve Mullins Alejandro Hernandez
Second Reader:	William Hatch

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE RECRUITING THE CYBER LEADER: AN EVALUATION OF THE HUMAN RESOURCE MODEL USED FOR RECRUITING THE ARMY'S "CYBER OPERATIONS OFFICER"	**5. FUNDING NUMBERS**
6. AUTHOR(S) Wallace C. Nicholson, Sean A. Gibbs	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/ MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.

12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

For the first time since the creation of the Special Forces branch in 1987, the Army authorized the creation of a new branch, the Cyber branch. With this, the Army joined the ranks of other organizations in this rapidly expanding arena. The Army found itself in a situation where it needed to quickly fill the positions required of this new branch. To accomplish this goal the Army developed a recruitment strategy based on the Army human resource management model.

The purpose of our research is to evaluate the effectiveness of that model to recruit Cyber Operations Officers and to examine the effects of its continued use. To perform this evaluation we conduct an operational assessment that included identifying and assessing measures of performance (MOPs) and measures of effectiveness (MOEs) based on data collected from: Army institutions; a survey of the Cyber Branch population; and the Person-Event Data Environment database. Our research also examined recruitment strategies and practices in other selected organizations to identify practical recommendations for improvements to current Army practices.

The results of this research suggest that while the Army was generally successful in accomplishing the identified tasks of its recruitment strategy, there were inconsistencies in its application. Additionally, through analysis of the survey data we were able to identify attributes that had the most impact on achieving desired effects. Finally, we found that the Army did not recruit in accordance with best practices for the cyber workforce and that it did not use available tools to measure aptitude in its recruitment and the selection process. We identify some practical implications and provide recommendations for further research in this fast-paced operational environment.

14. SUBJECT TERMS cyber, cyber operations, Cyber Operations Officer, human resource management, recruitment	**15. NUMBER OF PAGES** 177
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

RECRUITING THE CYBER LEADER: AN EVALUATION OF THE HUMAN RESOURCE MODEL USED FOR RECRUITING THE ARMY'S "CYBER OPERATIONS OFFICER"

Wallace C. Nicholson
Major, United States Army
B.A., Temple University, 2002

Sean A. Gibbs
Major, United States Army
B.S., Copin State University, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2017

Approved by: Steve Mullins
Thesis Co-Advisor

Alejandro Hernandez
Thesis Co-Advisor

William Hatch
Second Reader

Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

For the first time since the creation of the Special Forces branch in 1987, the Army authorized the creation of a new branch, the Cyber branch. With this, the Army joined the ranks of other organizations in this rapidly expanding arena. The Army found itself in a situation where it needed to quickly fill the positions required of this new branch. To accomplish this goal, the Army developed a recruitment strategy based on the Army human resource management model.

The purpose of our research is to evaluate the effectiveness of that model to recruit Cyber Operations Officers and to examine the effects of its continued use. To perform this evaluation, we conduct an operational assessment that included identifying and assessing measures of performance (MOPs) and measures of effectiveness (MOEs) based on data collected from Army institutions, a survey of the Cyber Branch population, and the Person-Event Data Environment database. Our research also examined recruitment strategies and practices in other selected organizations to identify practical recommendations for improvements to current Army practices.

The results of this research suggest that while the Army was generally successful in accomplishing the identified tasks of its recruitment strategy, there were inconsistencies in its application. Additionally, through analysis of the survey data we were able to identify attributes that had the most impact on achieving desired effects. Finally, we found that the Army did not recruit in accordance with best practices for the cyber workforce and that it did not use available tools to measure aptitude in its recruitment and the selection process. We identify some practical implications and provide recommendations for further research in this fast-paced operational environment.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

ACI	Army Cyber Institute
ACS	Army Cyber School
AMRG	Army Marketing Research Group
AR	Army Regulation
ARCYBER	Army Cyber Command
ASVAB	Armed Services Vocational Aptitude Battery
ASVAB-CT	Armed Services Vocational Aptitude Battery-Cyber Test
AVF	All-Volunteer Force
C2	Command and Control
CASL	Center for Advanced Study of Language
CATA	Cyber Aptitude and Talent Assessment
CCM	Cybersecurity Competency Model
CCoE	Cyber Center of Excellence
CF17	Career Management Field 17
CI	Counterintelligence
CMF	Cyber Mission Force
CPF	Cyber Protection Forces
CT	Cyber Test
CTE	Cyber Talent Enhanced
CWDT	Cybersecurity Workforce Development Toolkit
CWF	Cybersecurity Workforce Framework
CWFWR	Cybersecurity Workforce Framework Work Role
DA	Department of the Army
DCO	Defensive Cyber Operations
DHS	Department of Homeland Security
DMDC	Defense Manpower Data Center
DOD	Department of Defense
DoDI	Department of Defense Instruction
DOL	Department of Labor
DOPMA	Defense Officer Personnel Management Act

EFA	Exploratory Factor Analysis
ETA	Employment and Training Administration
F3ESA	Find, Fix, Finish, Exploit, Steady-state, and Assess
FAST	Flight Aptitude Selection Test
FORSCOM	Forces Command
GS	General Schedule
HRC	Human Resources Command
HRM	Human Resource Management
HRP	Human Resource Planning
HVI	High Value Individual
ICTL	Information/Communications Technology Literacy
JAGC	Judge Advocate General Corps
JAMRS	Joint Advertising, Market Research, and Studies
KSA	Knowledge, Skills, and Abilities
MDMP	Military Decision Making Process
MFR	Memorandum for Record
MHRM	Military Human Resource Management
MILPER	Military Personnel
MOE	Measure of Effectiveness
MOP	Measure of Performance
MOS	Military Occupational Specialty
MTOE	Modified Table of Organization and Equipment
NATO	North Atlantic Treaty Organization
NICE	National Initiative for Cyber Education
NIST	National Institute of Standards and Technology
NMF	National Mission Forces
NSA	National Security Agency
OCO	Offensive Cyber Operations
OCS	Officer Candidate School
OER	Officer Evaluation Report
OGLA	Officer Grade Limitation Act
OMB	Office of Management and Budget

OPA	Officer Personnel Act
OPM	Office of Personnel Management
PDE	Person Data Environment
PPB&E	Planning, Programming, Budgeting, and Execution
ROTC	Reserve Officer Training Corps
SANS	System Administrator, Audit, Network, and Security
SCI	Sensitive Compartmentalized Information
SHRM	Strategic Human Resource Management
SME	Subject Matter Expert
TRADOC	Training and Doctrine Command
TS	Top Secret
USAREC	United States Army Recruiting Command
USCYBERCOM	United States Cyber Command
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USMA	United States Military Academy
USSTRATCOM	United States Strategic Command
VTIP	Voluntary Transfer Incentive Panel

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We chose this research not only to fulfill our graduation requirements, but for its potential to be of some larger benefit to the Army as a whole. We are truly grateful for the support of our advisors, Steve Mullins, Alejandro Hernandez and William Hatch, during this process. Additionally, the numerous faculty members at the Naval Postgraduate School (NPS) were an invaluable resource as we navigated this intellectual terrain. Many other people and organizations contributed, big and small, to the completion of this product. The authors would like to specifically thank COL Eric Aslakson and LTC Benjamin Sangster for providing access and points of contact at the Cyber Center of Excellence (CCoE). Special acknowledgement also goes out to CW5 David Koscinch and Mr. Shawn Bova for their support with our survey distribution and help in understanding the selection process. From ARCYBER, we would like to thank Mrs. Nicole Camarillo, who put us in contact with key data sources for our research, to include CW5 John O'Reilly who was both knowledgeable and reliable on all things cyber. We would like to thank Human Resources Command - Cyber, specifically COL Timon Groves, CPT Thomas Schindler and CPT John Frank, for their assistance with the collection of data on the creation of the Cyber Branch and the recruitment process, the information and contacts they provided were invaluable to our research. COL William Lewis, Department of the Army G-1, took time out of his busy schedule to illustrate how difficult talent management in the Army actually is and the efforts that are being made to improve it. LTC (Ret) Jon Alt, MAJ Jarrod Shingleton and MAJ Nathan Parker from TRAC–Monterey are our heroes and deserve a special shout-out for the assistance they provided with our data analysis. Dr. Kathryn Aten helped us kick this off by assisting with the development of our survey, for which we are eternally grateful. Last but certainly not least, we would like thank our families. Without their unconditional love and unwavering support none of this would have come to fruition.

MAJ Gibbs would like to also thank MG Mitchell Kilgo, COL Brett Reister and COL (Ret) Joseph Hilfiker for helping him come up with a topic. A special acknowledgement goes out to COL Tim Watson for reminding me to always keep the warfighter in mind.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND—CYBER BRANCH

On June 23, 2009, Secretary of Defense Robert Gates directed the Commander of U.S. Strategic Command (USSTRATCOM) to establish U.S. Cyber Command (USCYBERCOM) (U.S. Strategic Command [USSTRATCOM], 2016). The Department of Defense (DOD) established USCYBERCOM to centralize cyberspace operations throughout the DOD in an effort to achieve effective command and control (C2), efficient organization of DOD cyber resources and synchronization between branches of service (Department of Defense [DOD], 2011). In anticipation of an eventual requirement to identify an appropriate service component to support USCYBERCOM, the Army created a cyberspace taskforce that led to the creation of Army Cyber Command (ARCYBER) in October 2010 (U.S. Army Cyber [ARCYBER], n.d.a.). ARCYBER's mission is "to support USCYBERCOM in its defense of DOD networks and the nation" (ARCYBER, n.d.).

In July 2011, the Department of Defense released the *DOD Strategy for Operating in Cyberspace*. This strategy outlines the initiative for DOD to treat cyberspace as an operational domain and to organize, train and equip the enterprise in order to operate effectively in this domain (DOD, 2011). In 2012, the DOD began building what is referred to as the Cyber Mission Force (CMF), which was created to carry out DOD's cyber missions. This CMF is DOD's investment in cyber personnel with the goal of being able to operate effectively in cyberspace. According to the DOD Cyber Strategy (2015), this CMF consists of 6,200 military, civilian and contractor personnel from across the military departments and defense components. These personnel are organized into 133 teams that included Cyber Protection Forces (CPF), National Mission Forces (NMF) and Combat Mission Forces (CMF). Each service component has a responsibility to provide personnel to these teams. The Army is specifically tasked with standing up 41 of these teams and their complementary National Support Teams (ARCYBER, 2016). The DOD reported on October 24, 2016, that all 133 of

USCYBERCOM's CMF teams have achieved initial operating capability (IOC) (DOD, 2016).

1. Creation of the Cyber Branch/17 Career Management Field

In September 2014, senior Army leaders authorized the creation of the cyber branch and the Career Management Field 17 (CF17) in support of USCYBERCOM's CMF requirement with an initial goal, according to Tice (2015), of building a population of 355 officers (Cyber Operations Officer–17A), 205 warrant officers (Cyber Operations Technician–170A) and 700 enlisted soldiers (Cyber Operations Specialist–17C). The purpose of this action, as outlined by a CF17 SME Panel conducted in September 2014, is to "create a new Army branch and career field focused on leading, planning and executing Offensive and Defensive Cyberspace Operations within Cyber Mission Force teams and in their respective C2 organizations" (Cyber Center of Excellence [CCoE], 2014, p. 5). In addition to the primary support provided to USCYBERCOM via CMF manning, this panel identified two other work role classifications that would be associated with the CF17: direct and specialized support to Cyber (CCoE, 2014). These other work role classifications provide the justification for additional personnel requirements outside of those specific to the CMF. This CF17 subject matter expert (SME) panel also established the 14 core work roles for the career field, proposed life cycle development, bridging strategies and a tentative timeline for execution (CCoE, 2014).

2. Recruiting the Cyber Operations Officer (17A)

With the strategy in place, in December 2014 the Army started recruiting officers for CF17 with a Voluntary Transfer Incentive Panel (VTIP) seeking the existing Army Officer Corps and a simultaneous in-service accessions campaign at West Point and ROTC programs to attract future Army officers (J. Frank, personal communication, May 4, 2016). According to the HRC Cyber Branch Career Manager, CPT John Frank, the initial recruitment process involved direct emails, Army Times articles, HRC Facebook and website advertising, in addition to pushing the word out to all the commanders of what would become Cyber formations (personal communication, May 4, 2016). As the process matured this responsibility was transferred to the Army Cyber School, which used a more targeted approach.

The Army Cyber School—established on August 4, 2013—created a single set of criteria to consider applicants for selection/transition into the Cyber Branch. These criteria were separated by rank, performance and skills/experience and evaluated individuals as either highly qualified, qualified or not qualified (Army Cyber School [ACS], 2017). The first VTIP resulted in the selection of 144 out of 740 applicants (19% selection rate) while the second VTIP resulted in the selection of 183 out of 662 applicants (28% selection rate), for a total of 327 out of 1230 applicants (27% selection rate) (CCoE, 2016). In-service accessions accounted for the commissioning of 32 17As in FY15 and another 32 in FY16 (J. Frank, personal communication, May 4, 2016).

This selection criteria/recruitment strategy is typical of the standard Army human resource management (HRM) model and as of March 3, 2017, has resulted in a 99% fill rate. However, the bottom line according to Harris and Morris (2016) and corroborated by multiple other sources, such as Arnold et al. (2013), Conti et al. (2015) and Schoka (2016), is that "the investment being made for structural facilities and institutional development will be of little value if we fail to make the necessary changes in how we conduct Talent Management of the Cyber Mission Force." These observations and the professional experiences of the two authors provided the motivation to understand and assess the Army's 17A recruitment program with a view to make constructive recommendations.

B. PROBLEM STATEMENT

The current human resource model used by the U.S. Army for recruiting Cyber Operations Officers may not adequately account for the unique requirements and attributes essential for providing highly technical leadership to cyber forces. The Army has already begun creating the force structure for the Cyber Branch as a whole, however; we propose that the recruitment and selection of cyber leaders with the appropriate combination of skill set and background to lead cyber operations has been less than optimal. We suggest that this stems from the Army's use of its standard HRM model to recruit these cyber leaders, prioritizing officers' leadership and operational experience over technical capabilities. As a result, a potential gap in technologically adept officers exists in the Army's newly created Cyber Branch.

C. PURPOSE OF THE STUDY

The purpose of this research is to 1) evaluate the effectiveness of the Army's current standard human resource model to recruit Cyber Operations Officers and to 2) examine some of the potential deleterious effects of its continued use. To support this, we will examine recruitment models in similar organizations (military/nonmilitary), conduct comparative analysis and recommend improvements to current practices. The effectiveness of the Army's human resource model used for recruiting Cyber Operations Officers directly affects the capabilities and effectiveness of the Cyber Branch and the Cyber Mission Force.

1. Research Questions

This thesis will answer the following questions:

a. Primary Research Question

- How does the Army's HRM for recruiting Cyber Operations Officers account for the technical skill set required to lead cyber forces?

b. Secondary Research Questions

- How does the Army recruitment strategy for Cyber Operations Officers balance manning requirements and individual capability requirements?

- How do Army Cyber Operations Officers' actual duties and responsibilities compare with expected/published duties and responsibilities?

- How do Army methods to measure the cyber leader aptitude compare to government and nonmilitary organizations with similar functions?

- What elements of nonmilitary HRMs for recruiting cyber leaders are feasible for implementation in an Army HRM to recruiting Cyber Operations Officers?

2. Potential Benefits and Limitations of the Study

The primary benefit of this study will be to increase understanding of the Army's human resource model for recruiting Cyber Operations Officers and whether or not it leverages best practices. In addition, it provides recommendations to improve the current Army HRM for recruiting Cyber Operations Officers (and possibly extensible to other officer specialty skill sets) that could positively impact military effectiveness.

This study will focus only on the Army HRM's impact on 17A officer recruitment. Other HRM elements (development/training and retention) will not be examined.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

This literature review provides the foundational knowledge and basic theoretical framework required to establish a scope for the evaluation of the human resource management (HRM) model used by the United States Army to recruit Cyber Operations Officers. This review examines the historical context of the Army's current HRM and the legislative actions that have shaped it. In addition, it considers specific low-density/ specialty populations within the U.S. military and discusses the role of the Army's human resource model in recruiting these individuals. This chapter concludes by outlining the DOD cyberspace workforce strategy and its alignment with the current Army strategy for recruiting Cyber Operations Officers.

A. ORGANIZATIONAL THEORIES AND FRAMEWORK FOR HUMAN RESOURCE MANAGEMENT AND RECRUITING

Evaluating the human resource model used by the U.S. Army to recruit Cyber Operations Officers requires a baseline understanding of some of the prevalent theories and frameworks that establish the parameters for the development and implementation of human resource models. Therefore, this research looks at the concept of Human Resource Management (HRM), the theories and frameworks that govern it, and how those frameworks shape human resource models currently used by organizations today. There is a wide range of information available on HRM—also referred to as strategic human resource management (SHRM) or human resource planning (HRP)—and its role in maximizing organizational performance. For our purpose, we will use the term HRM to refer to all human resource based management constructs and human resource models to address specific models of HRM.

1. HRM Definitions

As expected with a wide-ranging topic, there are multiple definitions, frameworks and descriptions of the HRM construct. A consistent theme in the definitions of HRM throughout the literature is the reciprocal relationship between an organization and its employees. Beer et al. (1984, p. 1) define HRM as "all management decisions and actions that affect the nature of the relationship between the organization and its employees—its human resources.” Storey (1995, p. 5) provides a more focused definition, calling HRM “a distinctive approach to employment management which seeks to achieve competitive advantage through the strategic deployment of a highly committed and capable workforce, using an integrated array of cultural, structural and personnel techniques.” The simplest and most direct definition of HRM is provided by Boxall et al. (2008, p. 2), who describes it as “The management of work and people towards desired ends.” This relationship between personnel and organizations is key in understanding HRM constructs and the human resource models that result from them. For our research we use Storey’s definition replacing “competitive advantage” with “strategic advantage.”

2. HRM Constructs: Soft and Hard

Storey (1989) highlights a key distinction in the relationship between personnel and organizations in his identification of the two primary approaches within the HRM construct: “hard” and “soft.” According to Storey, the hard HRM approach prioritizes organizational goals and regards employees as essential resources to achieve those goals, while the soft HRM approach prioritizes obtaining employee commitment through organizational strategies (Storey, 1989). According to Truss et al. (1997, p. 53), “the hard model is based on notions of tight strategic control and an economic model of man according to Theory X,” which argues that “people in general, dislike work, leading to tight managerial control through close direction” (Truss et al., 1997, p. 55).

By contrast the soft model was based on control of man through commitment and Theory Y—that “man will exercise self-direction and self-control in service of objectives to which he is committed” (Truss et al., 1997, p. 55). While these two approaches are categorically distinct, Storey claims they both share a common thread, “both versions share the presumption that decisions about the human resource are deserving of strategic attention because both start from the premise that the way in which this resource is managed will be critical to the success of the business plan” (Storey, 1992, p. 46). These HRM approaches were used to develop or, at a minimum, categorize the predominant human resource models found in the relevant literature on HRM. Additionally, they provide context for the strategic relevance of HRM on organizational outcomes that we will be observing in our research.

3. HRM Models

Some of the leading academic experts on HRM theories and frameworks include: Professor Emeritus of Management at the Stern School of Business at New York University, Charles Fombrun; Professor Emeritus of Business Administration at Harvard Business School, Michael Beer; Professor in Organizational Psychology and HR management at King's College of London, David Guest; and Professor of Human Resource Management at the Open University Business School, John Storey. They and their respective teams are responsible for creating the frameworks for four of the most recognized human resource models in HRM literature: the Michigan/Matching model, the Harvard model, the Guest model and the Storey model.

a. The Michigan/Matching Model

The Matching model—also referred to as the Michigan or the "hard" model—was created by Fombrun et al. (1984). This model holds that compatibility with organizational strategy should be a compulsory goal for the management of human resources and the organizational structure (Fombrun et al., 1984). This model emphasizes the importance of a tight fit between the HR strategy and the business strategy, prioritizing business strategy and regarding human resources like other resources, to be combined to achieve organizational goals. Evans and Lorange (1989) assert that the Michigan model is based on "product market logic" which infers that organizations marginalize labor to reduce cost and maximize profit. According to this model, there are three core elements required for organizations to function effectively: 1) Mission and Strategy, 2) Organization Structure and 3) Human Resource Management (Fombrun et al., 1984). The recruitment of personnel would fall under the third core element, human resource management, about which this model states, "People are recruited into the organization to do jobs defined by the division of labor…Performance must be monitored, and rewards must be given to keep individuals productive" (Tichy et al., 1982, p. 48). According to Cusworth and Franks (1993), while this model addresses external factors such as political, cultural and economical forces it fails to consider external influences such as situational factors, stakeholder interests and the notion of strategic choice, making it a flawed model.

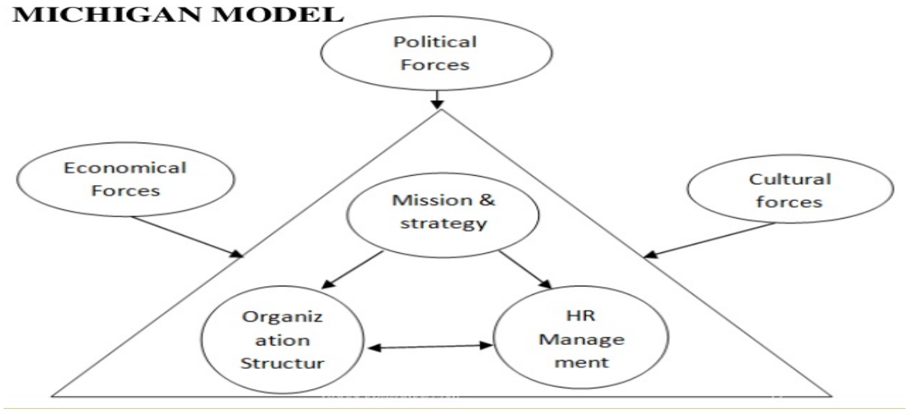


Figure 1. The Michigan/Matching Model. Source: Fombrun et al. (1984).

b. The Harvard Model

The Harvard Model, considered a “soft” HRM approach, was proposed by Beer et al. (1984) and emphasizes top management and their role in developing a relationship between the organization and its employees that satisfies the continuous changes in the needs of both parties. Beer et al. (1984) argue that this role is essential for an organization to effectively meet its obligations to its shareholders, employees, and society. As shown in Figure 2, this model identifies four HRM policy choices that define major HRM tasks that general managers must attend to: employee influence, human resource flow, reward systems and work systems (Beer et al., 1984). For our research, the human resource flow policy area is of particular interest. This policy area deals with managing the flow of people, to include, but not limited to: the recruitment and selection of employees, “personnel specialists and general managers must work in concert to ensure the personnel flow meets the corporation’s long term strategic requirement for the ‘right’ number of people and mix of competencies” (Beer et al., 1984, p. 9).

The Harvard Model also introduces what they refer to as the “Map of the HRM Territory” which could be used to assess the appropriateness or effectiveness of HRM policies. This map outlines two major considerations that influence HRM policies;

situational factors and stakeholder interests and two considerations that are influenced by HRM policies; HR outcomes and long-term consequences (Beer et al., 1984). The overarching premise of the Harvard model is that the organization's human resources are what gives them their competitive advantage and that ensuring that personnel are treated as assets and not costs is critical in achieving and maintaining that advantage.

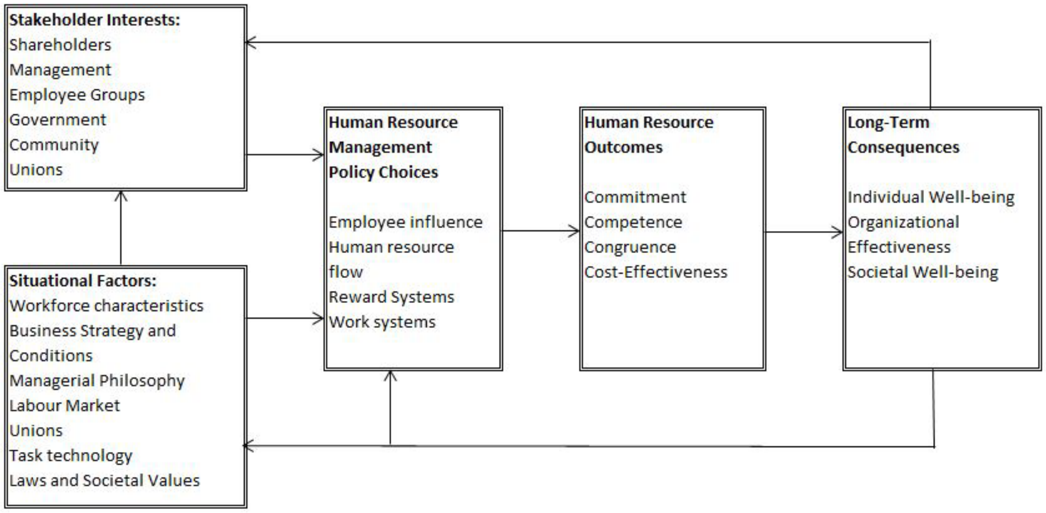


Figure 2. The Harvard Model of Human Resource Management.
Source: Beer et al. (1984).

c. The Guest Model

The Guest model, also considered a "soft" HRM approach, argues that the HRM is comprised of policies designed by management to maximize essential dimensions of an organization, to include organizational integration, employee commitment, flexibility and quality of work (Guest, 1987). In the article *Human Resource Management and Industrial Relations*, Guest outlines in great detail the components, challenges, features and concerns of these organizational dimensions. Of particular interest to our research, is Guest's (1987) quality of work dimension where he identifies three inter-related sub-dimensions: 1) quality of staff—which addresses the benefit of having organizational policies in place that prioritize the efficient and effective recruitment, development and retention of highly qualified staff; 2) quality of performance—which highlights the significance of establishing demanding goals and sustaining them through accountability; and 3) public image—which highlights the advantage of having an organizational reputation for distinctively treating employees well in the recruitment process (Guest, 1987). This model categorizes recruitment under the quality of work dimension and Guest emphasizes that it is essential to maintaining commitment, trust and motivation; ultimately maintaining the high quality of an organization.

d. *The Storey Model*

The Storey model proposes that HRM takes a comprehensive approach that includes a set of complementary policies based on a more rational abstract view (Storey, 1989). According to Storey (1992) this set of policies includes features such as placing appropriate emphasis on the value of human resources; that human resource decisions are a matter of strategic importance; that HRM has long-term implications on core performance of the organization and; that the management of certain critical HRM events—termed “key levers”—should be used to gain compliance and commitment. This model builds on the features of this view by identifying 27 points of difference between HRM and personal and industry relations categorized into four basic aspects, illustrated in Figure 3: beliefs and assumptions; strategic qualities; role of line managers and key levers (Storey, 1992).

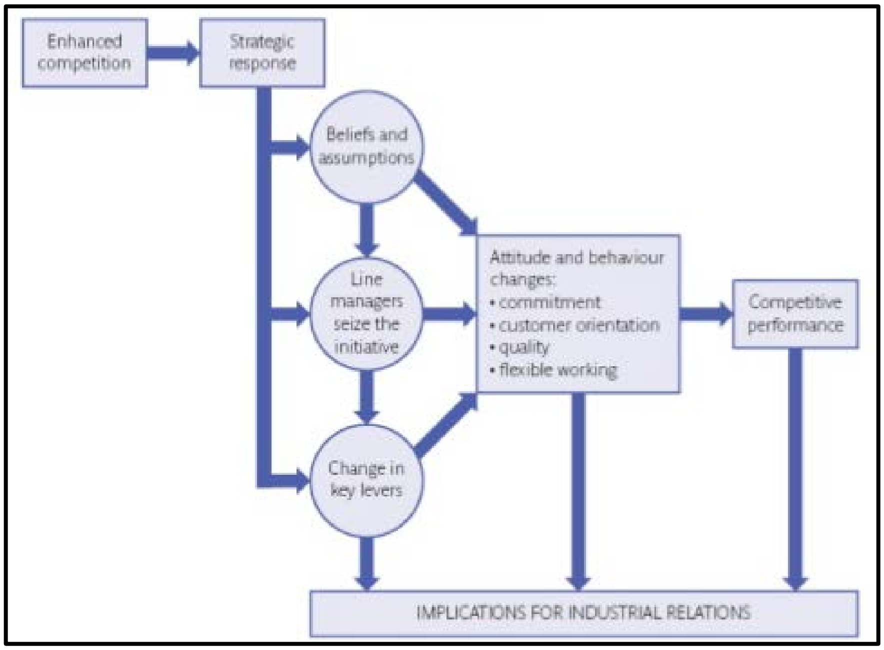


Figure 3. The Storey Model of the Shift to HRM Source: Storey (1992).

Critical to Storey's model is its distinction from conventional practice, with a less structure based process with more emphasis on the strategic role of the line manager and their responsibility to integrate business-management with people-management (Storey, 1992). For our research Storey's "key levers," which include "inflow into the organization" or recruitment, address the importance of this process and the significant impact it has on organizational success.

4. Analytic View of HRM Models

The work of these experts on this topic was a change from traditional personnel management and was conducted to add social scientific value to HRM and to facilitate "the development of testable hypotheses about its impact" (Guest, 1987, p. 503). Their work proved to serve its purpose, with many researchers developing and testing hypotheses based on these theories. A group of researchers in particular used some of these experts' work to argue what they considered to be a more empirically sound way to develop HRM models. Truss et al. (1997), accept that the two predominant constructs of HRM are the hard and soft versions, which "are based on opposing views of human nature and managerial control strategies." They conducted multiple case studies that led them to conclude that no pure examples of either approach exist and that, "the rhetoric adopted by the companies frequently embraces the tenets of the soft, commitment model, while the reality experienced by employees is more concerned with strategic control" (Truss et al., 1997, p. 55). The rhetoric referred to in their conclusion is basically the management's perspective or "top down" and the reality refers to the employee's perspective or "bottom up."

Truss et al. (1997) hypothesize that hard and soft versions of HRM could not coexist in a single HRM because of their conflicting perspectives on human nature and managerial control strategies. For this reason, Truss et al. believe that many of the prevalent HRM models are inherently contradictory because they contain elements of both hard, with the strategic integration dimension; and soft, with the employee commitment dimension (Truss et al., 1997).

Legge (1990) supports this argument, detailing specific contradictions in HRM models regarding the dual usage of the concept of integration. According to Legge, integration, when used in these HRM models, means both the integration with business strategy—what she calls "external fit"—and integration of reciprocal employment policies that aim at gaining employee commitment—what she calls "internal fit," making these models problematic and counterproductive to strategic objectives (Legge, 1990). Blyton and Turnbull provide a more practical explanation of this conflict, describing an alternate yet logical argument, purporting that employee commitment is secondary to business strategy not just because profit gains override HRM policy goals, but because even when "soft" aspects of HRM are prioritized it is only in anticipation of it having a positive impact on the business's bottom line (Blyton & Turnbull, 1992).

With this consensus, Truss et al. argue that for HRM constructs to be empirically and theoretically sound, they should be separated into two distinct concepts distinguished by the rhetoric—top down perspective—adopted by the organization and the reality—bottom up perspective—experienced by the employee (Truss et al., 1997). In other words, according to Truss et al., in order to have a complete HRM model it has to separately address both management and employee perspectives.

Noon (1992), concurs with Truss et al. (1997), Blyton and Turnbull (1992) and Legge (1990), and builds on their observations, arguing directly against Storey's HRM proposal. In contrast to Storey, Noon suggests the HRM construct is too comprehensive, built on ideas and proposals without explicit associated variables and hypotheses, stating, "The lack of general application of HRM 'theory' suggests that practitioners have some doubts or that its shortcomings in terms of testability prevent adequate empirical studies from being undertaken" (Noon, 1992, p. 28). Storey (1992), provides a defense for this argument, acknowledging room for debate in the area of non-explicit variables in his 27 points of difference. However, he disputes Noon's assertion that the "theory's" shortcomings should be measured in terms of testability, "Whether particular end-states can be attained, or will be attained, is perhaps not the main point" (Storey, 1992, p. 36).

According to Storey, the HRM model, regardless of its flaws and contradictions, was a result of necessity, facilitated by a desire for change to a conventional personnel management system that failed to adequately focus on the significance of competence and attitudes of employees (Storey, 1992). Storey adds that some nuance is required when discussing HRM, highlighting a point very similar to the two distinct concepts alluded to by Truss et al. (1997). This point, Storey (1992) insists, is that it is necessary to distinguish between HRM as a "style approach" adopted or preferred by management and HRM as a realized "pattern of relations" experienced by employees and that this distinction determines how the HRM should be examined.

5. HRM Models in Practice

In addition to reviewing the approaches to HRM and the predominant frameworks that most human resource models use, our research also inquires how these approaches and models appear in practice, and what additional types of specific HRM models currently exist beyond the four identified earlier. Becker and Huselid (1998, p. 55) describe the effective implementation and impacts of a HRM in the following way, "An internally consistent and coherent HRM system that is focused on solving operational problems and implementing the firm's competitive strategy is the basis for the acquisition, motivation, and development of the underlying intellectual assets that can be a source of sustained competitive advantage." This idea is largely agreed upon in HRM literature, however, approaches to accomplishing these ends differ significantly within the HR community.

Guest (1987) outlines four distinctive informal views, which he calls models, that he observed in his research of HRM best practices: 1) a human resource model; 2) a paternalist welfare model; 3) a production model; and 4) a professional model. This research of HRM best practices conducted by Guest and his research team at the London School of Economics was facilitated through a survey of senior managers with degrees in personnel management. This survey asks the 136 participants if there was a company which they or their organization categorized as having a good HRM model and what criteria they used to make that assessment (Guest, 1987). Guest and his team analyzed these criteria to create the four distinctive informal views of HRM best practices. The human resource model was characterized as being "people oriented throughout with an ethic of respect for the individual, maximization of individual talent…and clear challenging goals with feedback" (Guest, 1987, p. 508). Additionally, the paternalist welfare model is noted to have displayed a commitment to the customer that precipitated a deliberate process for the selection, training and treatment of employees. Next, the production model was said to be more closely aligned and integrated with business processes, highly structured with notable efficiency. Lastly, the professional model was identified by exceptionally qualified personnel managers fully integrated with line management forming a highly functional human resource team. According to Guest (1987), the major areas of distinction in these informal models are organization/business priorities; selection, quality and treatment of staff; and customer relations. The two models/views most relevant to our research are the human resource model and the professional model which both exhibited well-integrated policies and practices that resulted in the "maximization of individual talent" as a result of their recruitment process (Guest, 1987).

Storey also researched HRM models in practice. He and his team conducted case studies of 15 different companies separated into four different categories: the motor industry, public sector organizations, mechanical engineering and the process industry.

Storey and his team came up with three overarching conclusions: 1) companies were prioritizing employment management matters, 2) management was actively exploring employment management initiatives, 3) some degree of commonality of initiatives between companies across all four categories existed, and 4) commonality of initiatives did not inhibit variation between companies (Storey, 1992, p. 77). The results of Storey's research are in line with Guest's (1987), Storey (1992), however, uses the category of company vice a model/view to distinguish practices and he only addresses three of the four categories, based strictly on degree of variation with other categories.

For the motor industry, Storey and his team found that they prioritized team communications and functional flexibility; they found that process companies were using technology heavily, while neglecting managerial leadership and creating a more manageable employee supply (Storey, 1992). Still remaining were public sector organizations who were said to have an "infatuation with the tenets of the 'customer-facing' school of thought," meaning customer satisfaction drove business strategy which was prioritized over employee commitment (Storey, 1992, p. 79). The author went one step further with his research, providing a thematic analysis of the collected case studies. Of particular interest to our research was his analysis of the recruitment and selection process of these companies. Some of the highlights include: 1) companies treated the recruitment and selection process as a priority issue, 2) companies experimented with loosening of recruitment goals to increase the pool of potential candidates (i.e., non-standard work hours, increase in target age of recruits, special terms for woman), 3) companies advertised training and development opportunities—identified as the most crucial component of the process, 4) companies increased the use of aptitude testing designed specifically to assess candidate attributes, and 5) the traditional interview was the favored selection method among the companies they studied (Storey, 1992, p. 98).

While Guest and Storey researched HRM models in practice based on their respective frameworks, Moustroufas et al. (2015), propose a new HRM model, which they refer to as a competency profiling model. Competency models are not new, in fact David McClelland is credited with creating the competency movement in 1973 (Rodriguez et al., 2002). It can be argued competency models combine the best parts of the “soft” and “hard” HRM approaches: business strategy integration and employee commitment, “Organizations that select for competencies such as creative thinking begin to build a high-performance culture. Using competencies as the basis for staffing provides the flexibility needed to select and place individuals where they can best serve the organization” (Rodriguez et al., 2002, p. 310). Moustroufas et al. (2015) build on this concept by adding a profiling component to it. They use this model specifically as a tool for software engineers to establish a stratification of desired skills/capabilities that would allow them to prioritize potential candidates for Information and Communication Technology (ICT) companies and optimize their recruitment process and training programs (Moustroufas et al., 2015). The main argument behind the creation of this model is that the “identification, development and retention of skilled employees are the most important options for the company” (Moustroufas et al., 2015, p. 237). This model (Figure 4) consists of three areas of competence: 1) professional competences—composed of a basic set of skills essential for job responsibilities; 2) innovative competences—composed of a skill set essential for “continuous development, improvement and innovation”; and 3) social competences—which measures social capabilities for individual personality characteristics (Moustroufas, 2015, p. 237).

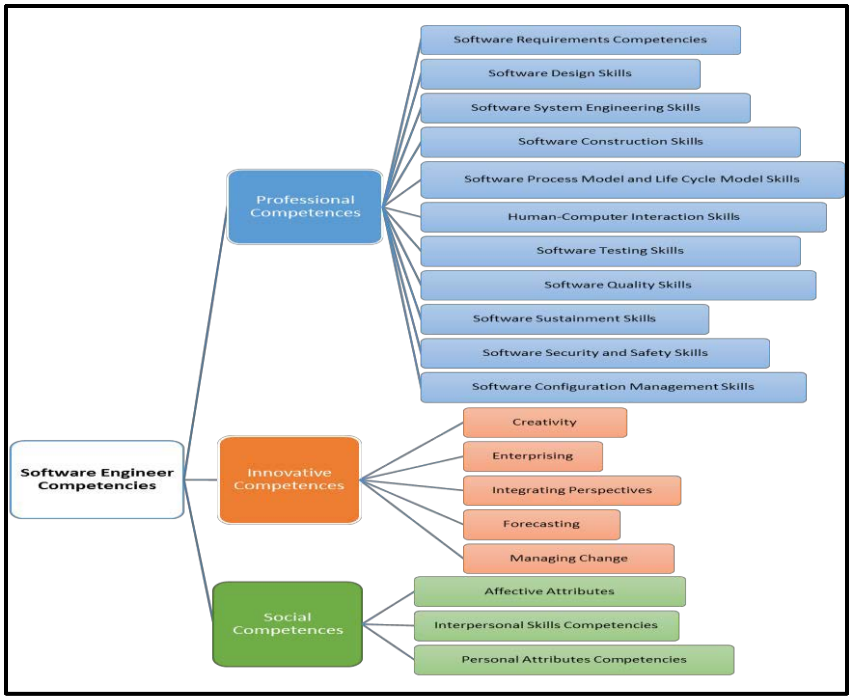

Software Engineer Competencies
Professional Competences
Innovative Competences
Social Competences
Software Requirements Competencies
Software Design Skills
Software System Engineering Skills
Software Construction Skills
Software Process Model and Life Cycle Model Skills
Human-Computer Interaction Skills
Software Testing Skills
Software Quality Skills
Software Sustainment Skills
Software Security and Safety Skills
Software Configuration Management Skills
Creativity
Enterprising
Integrating Perspectives
Forecasting
Managing Change
Affective Attributes
Interpersonal Skills Competencies
Personal Attributes Competencies

Figure 4. Level 1 and Level 2 of the Competency Model.
Source: Moustroufas et al. (1992).

Based on these areas of competence, Moustroufas et al. (2015) generated competency profiles that consolidate these three areas in each of the two following categories: 1) Required skills profile—specifies the requirements for a candidate seeking a specific position—and 2) Acquired skills profile—specifies the actual and obtained competencies of the employee. To validate this model and observe it in practice, Moustroufas et al. worked with two ICT companies in Greece. For this validation, a rating scale was created where they scored competencies from one to five, with five being the best score, the highest level and weighted value of the respective competency (Moustroufas et al., 2015). These researchers assert that this rating scheme provides an organization with the ability to measure the gap between the two competency profiles of required and acquired skills, ultimately enhancing the organization's selection process of potential candidates (Moustroufas et al., 2015). While the research conducted by Moustroufas et al. on the competency profiling model was limited to two companies, they found that the model was a useful tool that could significantly benefit HRM (Moustroufas et al., 2015).

As our research looks at the HRM model being used for the recruitment of a highly technical military career field, this competency profiling model provides a substantial amount of relevant context to consider, to include how it is validated and used in practice, specifically how it identifies skilled individuals for recruitment. We will revisit this idea of competency profiles in our conclusion.

6. Assessing Effectiveness of HRM Models

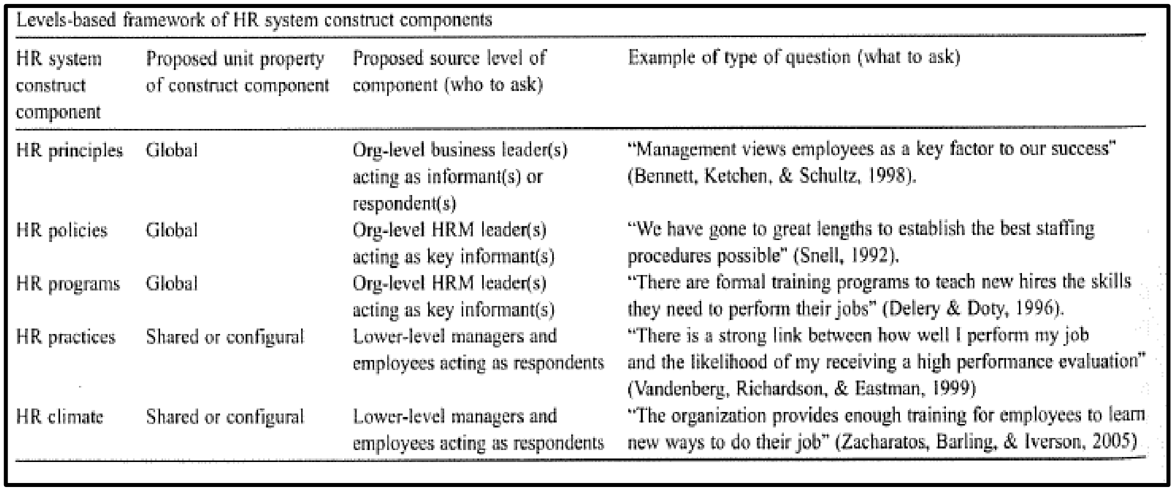
The theoretical bases of most approaches for the HRM focus on the Human Resource (HR) systems of an organization to understand the correlation between the HRM and organizational performance. Based on existing literature on HRM, there are five components of the HR system used to assess the effectiveness of an HRM: 1) Principles, 2) Policies, 3) Programs, 4) Practices and 5) Climate (Arthur & Boyles, 2007). Arthur and Boyles (2007) define each of these components and provide metrics for establishing the weight of each and its correlation to organizational performance.

While all are relevant to the overall assessment of the effectiveness of the HRM, each one represents an element that independently impacts the HRM and can shed light on organizational performance. The HR systems that have the most relevance for our research are HR Programs, which is defined as, “the set of formal HR activities used in the organization” and HR practices, which is “the implementation and experience of an organization’s HR programs by lower-level managers and employees” (Arthur & Boyles, 2007, p. 80). The recruitment process straddles both the HR programs and practices of the HR system as it impacts both the organization/management and the individual employee. This research will focus only on observations from these two HR systems to evaluate the effectiveness of the HRM model used by the U.S. Army in its recruitment of 17As.

In describing how to assess the effectiveness of HRM models, Arthur and Boyles (2007) outline two predominant considerations to account for during the assessment: “levels-based construct properties” and “applications of levels-based concepts.” This idea of “levels-based construct properties,” refers to understanding the behavior in organizations that have distinctly different groupings of individuals or collections of individuals and properly accounting for this behavior in the assessment. Arthur and Boyles (2007, p. 81) emphasize that failing to do so could result in either a "level-based misspecification"—which happens when an observed effect is incorrectly applied to a level other than the one represented in the evaluation—or a "unit-level construct property and aggregation issue"—which occurs when data collected from individuals are presented in a way that allow them to be misinterpreted and analyzed as organizational data without acceptable conditions for aggregation. Both of these potential issues directly impact the validity of the evaluation.

In considering "applications of levels-based concepts" Arthur and Boyles (2007) explain the value of gaining an understanding of the levels-based construct, and how it improves the insight of researchers into the validity and reliability of the data they are collecting and analyzing. One of these insights is in reference to the "inter-rater reliability/multiple respondent debate" which addresses two sides of an argument that disputes the value of individual raters versus multiple raters on the inter-rater reliability of the HRM assessment (Arthur & Boyles, 2007, p. 83). For context, inter-rater reliability "provides a way of quantifying the degree of agreement between two or more [raters] who make independent ratings about the features of a set of [respondents]" (Hallgren, 2012, p. 23). One side of this argument, presented by Gerhart et al. (2000), suggests, logically, that having multiple raters with single-respondent measures of HR practices would increase inter-rater reliability. The other side of the argument, claimed by Huselid and Becker (2000), is that having a knowledgeable individual rater provides greater validity and reliability to data collected for analysis than having multiple respondents with limited knowledge on an organization's HR programs. Citing Gerhart et al. (2000) and Huselid and Becker's data, Arthur and Boyles (2007) offer that both authors are correct and that the real issue is the misalignment between what is being assessed—in this case HR programs and practices—and at what level it is being assessed—organizational or individual employee levels. This misalignment impacts inter-rater reliability much greater than the number of raters involved in the evaluation (Arthur & Boyles, 2007).

Additionally, in considering “applications of levels-based concepts,” Arthur and Boyles (2007, p. 84) introduce “levels-based guidelines for strategic HRM research” that provide recommendations for the assessment of HRM models. These guidelines focus primarily on organizational surveys, and offer practical solutions for “whom to ask” and “what to ask” to best represent the HR system component being assessed. In outlining the guidelines for effective assessments Arthur and Boyles identify HR programs as a collective-level construct that originates from the organizational level and can be easily observed through publicly available data and/or access to archived records (Arthur & Boyles, 2007). Following that, HR practices were identified as an individual-level construct that originates from “shared or configural properties of individual employee experiences and perceptions” (Arthur & Boyles, 2007, p. 84). With levels-based constructs defined, Arthur and Boyles (2007) point out appropriate steps to take to determine whom to ask and what to ask, Figure 5 depicts the basic framework of these guidelines. Our research is most concerned with observing the HR Programs and Practices components of the HR system to evaluate the effectiveness of the Army’s HRM model for recruiting the Cyber Operations Officer.



Levels-based framework of HR system construct components

HR system construct component	Proposed unit property of construct component	Proposed source level of component (who to ask)	Example of type of question (what to ask)
HR principles	Global	Org-level business leader(s) acting as informant(s) or respondent(s)	“Management views employees as a key factor to our success” (Bennett, Ketchen, & Schultz, 1998).
HR policies	Global	Org-level HRM leader(s) acting as key informant(s)	“We have gone to great lengths to establish the best staffing procedures possible” (Snell, 1992).
HR programs	Global	Org-level HRM leader(s) acting as key informant(s)	“There are formal training programs to teach new hires the skills they need to perform their jobs” (Delery & Doty, 1996).
HR practices	Shared or configural	Lower-level managers and employees acting as respondents	“There is a strong link between how well I perform my job and the likelihood of my receiving a high performance evaluation” (Vandenberg, Richardson, & Eastman, 1999)
HR climate	Shared or configural	Lower-level managers and employees acting as respondents	“The organization provides enough training for employees to learn new ways to do their job” (Zacharatos, Barling, & Iverson, 2005)

Figure 5. Levels-based Framework of HR System Construct Components.
Source: Arthur and Boyles (2007).

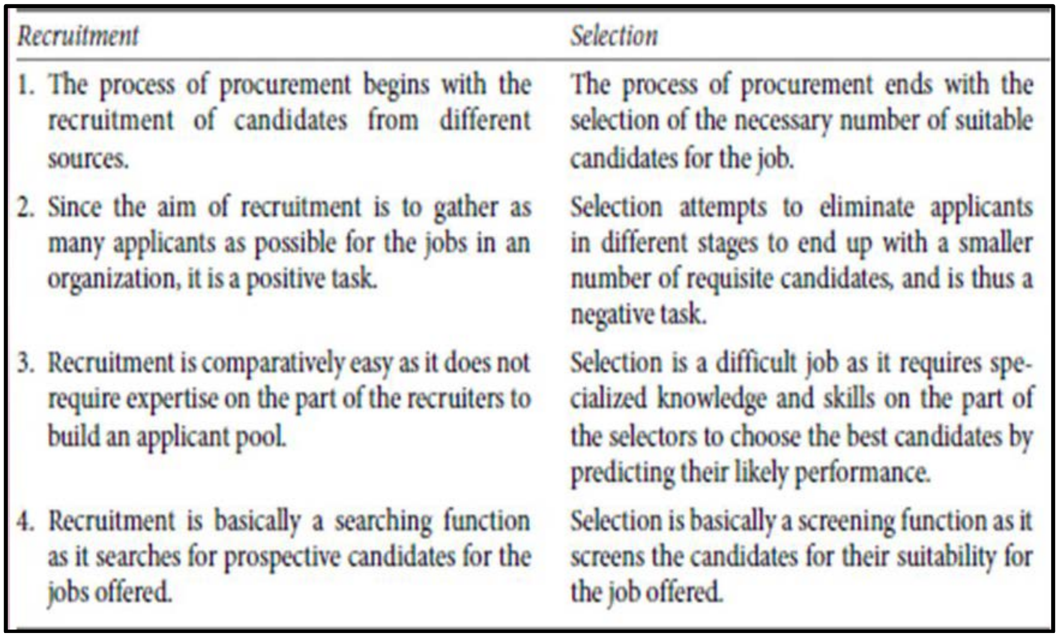
In summary, to assess the effectiveness of HRM models Arthur and Boyles (2007) recommend that researchers understand the levels-based construct of the HR system components being observed (individual or collection of individuals), avoid misspecification of levels, avoid misalignment of levels and HR system components, and base “whom to ask” and “what to ask” on explicit levels-based rationale. By focusing on HR components to measure how HRM models impact organizational performance, Arthur and Boyles provide an empirical solution to evaluating the effectiveness of HRM models. This thesis builds on portions of what Arthur and Boyles outline in this solution.

7. Recruitment Strategies: Recruitment and Selection

Regardless of which HRM approach, framework or model one applies, recruitment is identified as a critical part of it. In the Michigan model, it is part of the third “core element,” for the Harvard model it is part of the “human resource flow,” for the Guest model it is part of the “quality of work” dimension and in the Storey model it is one of the “key levers.”

With such a variation in the application of this term we find it necessary to provide a baseline definition. For this research, we follow Lewis, and the term recruitment will refer to “the activity that generates a pool of applicants, who have the desire to be employed by the organization, from which those suitable can be selected” (Lewis, 1985, p. 29). Generating a pool of applicants is key to a recruitment strategy, however it is only one half of the process, the other half is “selection,” a term often confused with recruitment (Rashmi, 2010). Iles and Salaman (1995) note that the acknowledgement of recruitment and selection as “integrated key tasks” for an organization’s HRM model is one of the most important concepts of Storey’s “key levers.” However, it also noted that the distinction between the two must be fully understood. For that purpose, we also provide a baseline definition for selection, which in this research will refer to “the process of differentiating between applicants in order to identify (and hire) those with a greater likelihood of success in a job” (Stone, 1989, p. 173). Additionally, Table 1 details what, according to Durai (2010), are some of the key distinctions between recruitment and selection.

Table 1. Difference between Recruitment and Selection. Source: Durai. (2010).



Recruitment	*Selection*
1. The process of procurement begins with the recruitment of candidates from different sources.	The process of procurement ends with the selection of the necessary number of suitable candidates for the job.
2. Since the aim of recruitment is to gather as many applicants as possible for the jobs in an organization, it is a positive task.	Selection attempts to eliminate applicants in different stages to end up with a smaller number of requisite candidates, and is thus a negative task.
3. Recruitment is comparatively easy as it does not require expertise on the part of the recruiters to build an applicant pool.	Selection is a difficult job as it requires specialized knowledge and skills on the part of the selectors to choose the best candidates by predicting their likely performance.
4. Recruitment is basically a searching function as it searches for prospective candidates for the jobs offered.	Selection is basically a screening function as it screens the candidates for their suitability for the job offered.

Beer et al. (1984) provide insight on the importance and impact of recruitment decisions on an organization, explaining how basic choices for where and how to recruit affect the makeup of the workforce, the culture of the workforce and employee turnover. Additionally, they posit that the common issues with the recruiting of professional and technical talent stem from the failure of academic institutions to provide qualified candidates. Iles and Salaman (1995) counter this argument citing Rynes and Barber's (1990, p. 289) analysis of enhancing recruitment efforts, "organizations can attempt to change their recruitment practices, change the inducements or incentives offered to applicants, or widen their recruitment net to target 'non-traditional' sources" Iles and Salaman also introduce a psychological aspect of recruitment, highlighting that recruitment is the first phase in a process where a potential employee and organization are communicating, deciding on whether the other meets their expectations, and whether or not they want to go to the next stage of this process (Iles & Salaman, 1995).

On the practical side of recruitment analysis Geetika describes what he calls "dimensions of recruitment strategies:" "whom to recruit;" "from where to recruit;" and "how to recruit" (Geetika, 2007, p. 8). Geetika (2007) explains that when deciding on "whom to recruit," organizations have to choose between creating a larger pool of potential candidates with less skill and investing in training and education programs or investing in labor costs/employee compensation packages to attract highly skilled candidates. Next, he writes that to determine "where to recruit from," organizations should simply look into markets where there are higher populations of job seekers. Finally, Geetika offers that "how to recruit" refers to either internal or external recruitment methods, e.g., promotions and transfers for internal and advertising and job fairs for external (Geetika, 2007).

Iles and Salaman (1995) explore specific recruitment options with the goal of attracting candidates to the organization. These options include recruitment literature, informal word-of-mouth recruiting and "targeted" recruitment practices (Iles & Salaman, 1995). The authors discuss the impacts of different types of recruitment and how, depending on the organization's approach, some recruitment options can be counterproductive. One example is informal recruiting practices analogous to social media interactions, "informal recruiting practices may reduce diversity and encourage the recruiting of 'like by like,' perhaps inhibiting creativity, as well as ensuring that sections of the community which are currently under-represented in an organization's workforce remain so" (Iles & Salaman, 1995, p. 211). Armstrong (2006) identifies more standard recruitment options to include: advertising, e-recruitment, outsourcing and partnerships with academic institutions. Outsourcing and partnerships with academic institutions are of particular interest to our research. Outsourcing recruitment, according to Armstrong (2006), is a time saving option that allows organizations to use professional recruitment agencies to attract and supply suitable candidates to the pool of applicants. This is an option most appropriate for organizations attempting to recruit specialty skill sets into newly created organizational roles in a relatively short period of time. Beer et al. address the partnerships with academic institutions option, recommending the following coordination initiatives: placing facilities near partner academic institutions; providing partner academic institutions with forecasted work roles and desired skill sets; assigning key executives to staff partner academic institutions; and internship programs (Beer et al., 1984). This option is most appropriate for organizations making a long-term investment in the makeup of its workforce.

Rashmi (2010) outlines another practical concept, describing three interrelated stages of the recruitment process: 1) planning, 2) strategy development, and 3) evaluation of processes. This concept continues with the description of the planning stage as where employment opportunities are translated into target goals that define the parameters for the pool of applicants. Next, strategy development is described as when a decision is made on "how, where and at what cost to look for suitable candidates" (Rashmi, 2010, p. 24). Lastly, the author adds that the evaluation of processes is continuous and its purpose is to reduce cycle times and incurred costs. An important consideration introduced by Rashmi's stages of the recruitment process is the defining of the parameters for the pool of applicants. These parameters control the size of the applicant pool and indicate that the organization and its managers understand the type of candidates they are looking to attract and how many (Rashmi, 2010).

Part of defining parameters for the applicant pool is defining requirements, which is an essential element of the recruitment process. Armstrong (2006) argues that not only should these requirements be specified in the recruitment process but that they be justified in accordance with the organization's HRM model. Armstrong outlined several approaches to defining requirements for the recruitment pool. The first he calls a "person specification," that identifies eight categories used to describe candidate requirements: technical competencies, behavioral and attitudinal requirements, qualifications and training, experience, specific demands, organizational fit, special requirements, and meeting candidate expectations (Armstrong, 2006, p. 411). The author identifies three additional approaches with similar concepts for defining requirements including: the Rodger's (1952) "seven-point plan" the "fivefold grading system" and the "competency-based approach." According to Armstrong (2006), using these types of approaches provides organizations with the basic information required for implementing a recruitment strategy and establishes the foundation for the selection process.

Selection, which is sometimes paired with assessment and/or appraisal in HRM literature, adds another complementary, yet distinct and equally impacting, element to the recruitment strategy, best summarized by Iles and Salman as

> In principle, and also in effect, the contemporary processes of selection and assessment represent the moment organizational restructuring meets and impacts on individuals, either as putative or actual employees, and in so doing, defines, understands, and assesses them in terms of organizationally defined critical qualities, and is the site of individual entry into—or rejection from—newly defined organizational roles. (Iles & Salman, 1995, p. 204)

In other words, selection is the gateway into an organization and the gatekeepers have a list of who they want to hire and a method for authorizing entry. As described in the definition, selection differentiates applicants based on the probability of their success, a probability, in most cases, defined by organizational processes. Iles and Salaman (1995) expand on this idea by emphasizing that the selection process should be seen in terms of its interaction with organizational expertise and power structure, not efficiency or logic. Townley (1989) adds that, by definition, the selection process is discriminatory and highlights the tendency of organizational management to emphasize employee "acceptability," in regards to management, over "suitability" identified by job requirements.

These organizational processes/methods are prevalent throughout literature on HRM and recruitment and no universally accepted standard was evident in our research. Some authors like Armstrong (2006) suggest there are as few as three processes/methods involved in selection, while others like Rashmi (2010) suggest as many as seven. These processes/methods include formalities that span from interviews to checking references, all with the intent of distinguishing applicants from the recruitment pool. While no standard was observed in our research we found that the most predominant selection methods are interviews and tests.

Armstrong (2006) identifies three types of interviews: individual interviews, interviewing panels and selection boards, outlining each of their distinct advantages and disadvantages. The author goes on to describe the purpose of interviews as a forecasting tool that collects and assesses information about a potential employee that can be used to determine job performance (Armstrong, 2006). Consensus throughout literature on this topic is that the interview is one of the most consequential methods of the selection process, “Any selection process is rarely complete without a personal interview” (Rashmi, 2010, p. 86).

With regard to selection tests, Rashmi (2010, p. 89) identifies four types: “ability tests,” “personality tests,” “group situational tests” and “work simulation tests.” Ability tests include both achievement and aptitude tests, and according to Rashmi (2010), achievement tests measure job related competencies in skills already held by potential candidates. While aptitude tests measure a candidate’s potential for attaining job related competencies through training (Rashmi, 2010). The three remaining types of selection tests identified by Rashmi represent more abstract approaches to testing potential employee candidates and are outside of the scope of our research. Arthur (2006) identifies five selection tests: intelligence, personality, ability, aptitude and attainment, four of which align perfectly with Rashmi’s (2010) four types. Arthur (2006), however, adds a distinction to these tests by categorizing them as either psychometric tests or psychometric questionnaires. The distinction being that tests have correct answers and performance is measured by the scores, whereas questionnaires assess performance but the scores identify characteristics and/or qualities of the candidate (Arthur, 2006). According to Arthur (2006), the purpose of these psychometric evaluations (tests or questionnaires) is to provide an organization with a tool to objectively assess a candidates character and abilities in order to predict the probability of success in a given job or role. Selection tests, like interviews appear to be valuable tools for effective recruitment strategies.

B. REVIEW OF HRM FOR RECRUITING IN SIMILAR ORGANIZATIONS

To understand how the U.S. Army recruits Cyber Operations Officers, we must first examine the personnel requirements that drive recruitment priorities. Federal workers, military and non-military, are classified by the type of work performed, the level of expertise, and the level within the organizational structure. Based on the attributes necessary to provide the required functions or capabilities, government and military organizations formulate a list of recruitment priorities. While operational needs are the primary drivers for the compilation of key attributes of federal labor, force structure and legal authority significantly influence the recruitment of personnel. Legal authorities play a greater role on desired and required attributes of the workforce within DOD, while force structure governs the number of personnel recruited.

1. The Office of Personnel Management (OPM)

The Office of Personnel Management (OPM) "works in several broad categories to recruit, retain, and honor a world-class workforce for the American people." (OPM, 2017). Through a variety of programs and initiatives, OPM recruits and acquires personnel with general or narrowly defined skill sets based on labor needs of federal agencies. OPM focuses on the facilitation of job searches, employment accessibility, provision of benefits, and talent retention. (OPM, 2017). The organization is responsible for policy development to support HRM within federal agencies and standardize process across the federal government. The classification and qualification policies form the backbone of OPM's guidance. Detailed information about classification processes, occupational definitions, and grade criteria are directly tied to Federal Wage Classification Systems and job standards. (OPM, 2017). "Position classification standards and functional guides define federal white-collar occupations, establish official position titles, and describe the various levels of work." (OPM, 2017). The General Schedule (GS) is the predominant pay scale for white collar Federal employees. Over 1.5 million people fall under the GS pay scale. GS and white collar are often used interchangeably. (OPM, 2017). Trade, craft, or labor occupational series outlined in the *Handbook of Occupational Groups and Families* are compensated through the Federal Wage System. (OPM, 2009a). The handbook provides definitions for GS and Federal Wage occupational codes. White collar positions possess series numbers 0000 through 2200. Trade, craft, or labor positions have series numbers between 2500 and 9000. Occupational codes are further subdivided into specialties to provide agencies more flexibility. The specialties are referred to as parentheticals. (OPM, 2009b). The *Introduction to the Position Classification Standards* goes into greater detail on the GS Classification System for white collar occupations. (OPM, 2009b). The general characteristics of work classifiable under the GS are professional work, administrative work, technical work, and other kinds of work. (OPM, 2009b). Professional, administrative, and technical work require a bachelor’s degree or the training equivalent of a bachelor’s degree. Because the nature of this thesis research concerns only Army Officers, the remaining study of Federal workers will be confined to GS employees for comparative analysis.

Recruitment of Federal employees is based on the aforementioned classification and qualification process. USAJobs.gov is the primary inject point for individuals seeking civilian Federal employment. (OPM, 2017). An applicant completes an application online and awaits contact from the advertiser of the position. OPM provides the platforms for agencies to recruit externally. Development of personnel and internal recruitment is a responsibility of the individual agencies. (OPM, 2017). There are individual development programs available for civilian Federal workers, but not on the same scale as the military. Education and training programs, with the exception of functions unique to the Government, are few compared to the size of the workforce. Development of competencies is more of an individual responsibility. OPM policies and regulations cover position requirements and the mechanisms for acquiring (and compensating) individuals with requisite competencies. Programs for continuing education or expanded training opportunities do not exist in the same proportion as in the DOD. There are five training statutes, two executive orders, and two policies from Office of Management and Budget (OMB). (OPM, 2017). The executive orders are much older than the statutes, dating back to 1967 and 1999 respectively. The statues, while more recent, lay much of the burden for training and development programs on the agencies. This was done to provide more flexibility with talent management, classification, and grading. (OPM, 2017). Position and job specific training programs are managed at the agency level, with management, supervisory, and acquisition being the exceptions.

2. The Federal Civilian Workforce

The process for how the civilian Federal workforce matches personnel against the requirements under Government functions was explained in the previous paragraphs. Our examination now turns to civilian Federal employee functions most analogous to Army Cyber Operations Officers. Occupational series 2210, Information Technology

Management, and the accompanying specialties align with Signal and Cyber branches of the Army. (OPM, 2009a). The 2210 specialties focus mostly on operation and maintenance of IT. There are two specialties associated with security, information security and network security, respectively. There are no specialties for offensive cyber capabilities in the civilian occupational inventory. (OPM, 2009a). The Federal Cybersecurity Workforce Strategy, published in July 2016, seeks to identify the cybersecurity workforce within the Federal Government and recruit externally from a labor pool of qualified individuals. (OMB, 2016). OPM launched a website, Cybercareers.gov, to specifically recruit internally and externally for individuals with the technical competence for a career in cybersecurity.

"The Employment and Training Administration (ETA) has worked with the Department of Homeland Security and the more than 20 federal departments and agencies that make up the National Initiative for Cybersecurity Education (NICE) to develop a comprehensive competency model for cybersecurity." (National Institute of Standards and Technology [NIST], 2017). The Department of Labor (DOL) uses the Cybersecurity Competency Model (CCM) to define the attributes necessary for personnel that perform cyber functions and activities within the federal government. (NIST, 2017). The non-military federal cybersecurity workforce is organized into seven categories under the Cybersecurity Workforce Framework (CWF). The CWF, in order from general to specific, consists of Specialty Areas. Specialty areas are further subdivided into Work Roles with definitions to provide organizations with specificity in classification of the Cybersecurity Workforce. (NIST, 2017). It "provides a common language to speak about cyber roles and jobs and helps define personal requirements in cybersecurity." (NIST, 2017). The categories are Analyze, Collect and Operate, Investigate, Oversight and Development, Protect and Defend, and Security Provision. (NIST, 2017). Work Roles and their definitions are contained in the Cybersecurity Workforce Framework Work Role (CWFWR) table. (NIST, 2017). The National Institute of Standards and Technology (NIST) created the Cybersecurity Workforce Development Toolkit (CWDT) to assist organizations with understanding the posture of their cybersecurity workforce and staffing needs (NIST, 2017).

The legal authorities under which non-military and non-DOD federal agencies operate also impact recruitment methods and priorities. The most salient difference between DOD and non-DOD entities is that the former has the legal authority to conduct offensive cyber operations (OCO) under Titles 10, the role of armed forces in the United States, and 50, the role of War and National Defense, of the United States Code. The Department of Homeland Security's (DHS) authority stems from title 6 and others based on the child agencies under the DHS umbrella. For example, the Coast Guard, which is subordinate to DHS, operates under Titles 6, 10, 14, 19, 33, and 46. These legal authorities further refine which skills and attributes an organization requires within the CWF.

Force structures within federal agencies are customarily created, abolished, and modified through an act of Congress. Congress delegates presidential reorganization authority to the Executive Branch for limited periods of time to make changes that could not be realistically achieved through the congressional process. (Hogue, 2012). In conjunction with budgetary restraints, the President makes modification to government agency force structure via executive orders. Historically, small modifications impact the number of personnel that perform a particular function. (Hogue, 2012). Substantial and sweeping modifications to force structure, such as creation or elimination of a government function, influence both the number and type of personnel in the federal workforce. These legal authorities further refine which skills and attributes an organization requires within the CWF.

The President develops "plans for reorganization of portions of the federal government and to present those plans to Congress for consideration under special parliamentary procedures. Under these procedures, the President's plan would go into effect unless one or both houses of Congress passed a resolution rejecting the plan, a process referred to as a 'legislative veto.'" (Hogue, 2012, p. 1). The new force structure informs the recruitment and manning strategy for the affected agencies.

3. Non-government Civilian Organizations

Civilian organizations tend to favor “soft” HRM models. The models that we observed lie on a scale between the Harvard Model and the Guest Model. Non-military and civilian organizations operate in cybersecurity labor environment with a near 0% unemployment rate for targeted demographic (Morgan, 2015). Therefore, organizations must focus on employee wants and needs to recruit and retain workforce with critical specialized skills. For the purposes of this research, recruiting models of Facebook and Google are examined.

Dr. John Sullivan, Professor of Management at San Francisco State University, produced case studies on the talent management practices for both companies. Facebook quantifies employees and recruits in terms of added economic value to the organization (Sullivan, 2013). “When a single engineer is worth up to $1 million, you strongly invest in recruiting and in increasing their productivity, and you certainly don’t focus on the relatively miniscule cost per hire that it takes to recruit them” (Sullivan, 2013). Evaluating personnel as assets that bring revenue into the organization allows Facebook to identify which attributes high performers possess, how to nurture those skills, and predict return on investment.

Google, on the other hand, takes a volume approach to recruiting. The positions themselves become recruitment tools (Sullivan, 2005). The company employs a large number of contracted recruiters. So much so, that recruiters focus on different company functions or demographics (Sullivan, 2012). Similar to Facebook, Google leverages the analytics capabilities of their technology to assist with recruiting (Sullivan, 2012). An army of recruiters has allowed Google to reduce the amount of time between application and hiring. What is more revealing, though, is how Google assesses talent. Credentials are simply not enough. Their interview process uses behavioral interviews centered around specific situations to determine how prospective recruits will employ their skills and experience to solve a problem (Nisen, 2013). Both Facebook and Google integrate elements from the Harvard and Guest models to establish policies to improve employee relationships, which ultimately leads to the accomplishment of organizational goals. Facebook also incorporates some elements of hard constructs. The quantification of human capital in terms of additional monetary assets is used to assess a recruit’s value, and potentially reduce labor costs.

4. DOD and the U.S. Army

Due to the authorities under which DOD operates, the classification of both civilian and military personnel differs from the non-DOD federal workforce in both small and significant ways. DOD Directive 1400.5 states that is “policy to use civilian employees in all positions that do not require military incumbents for reasons of law, training, security, discipline, rotation, or combat readiness, or that do not require a military background for successful performance of the duties involved” (DOD, 2005a). The management of civilian DOD personnel used in the aforementioned positions is covered by DOD Directive 1400.25 (DOD, 2003). Classification of civilian DOD employees uses the descriptions and definitions published by OPM and the CWF. However, additional documentation is used for roles and responsibilities directly tied to title 10 authority. DOD 8140.01 “unifies the overall cyberspace workforce and establishes specific workforce elements (cyberspace effects, cybersecurity, and cyberspace information technology (IT)) to align, manage and standardize cyberspace work roles, baseline qualifications, and training requirements. This directive does not address operational employment of the work roles” (DOD, 2015a). Roles and responsibilities are defined in DOD Directive 8570.01M, which is now a reference to DoDD 8140. (DOD, 2015b). It should be noted that the Cybersecurity Workforce is one of the few occupations standardized at the DOD level, along with legal and intelligence functions.

Army recruitment policy starts with guidance from DOD. Organizations and positions within those organizations responsible support to service level recruitment are identified within directives and issuances. DOD level policy for recruitment within the respective services is confined to resourcing and reporting requirements. The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) is responsible for ensuring the services “use the most efficient and cost-effective processes in the Military Services’ recruitment of new personnel” (DOD, 2008). DOD Instruction 1304.32 outlines reporting requirements on service level recruitment programs to support the planning, programming, budgeting, and execution (PPB&E) process (DOD, 2011). "The Secretary of the Army as the DOD Executive Agent for the acquisition, maintenance, and disposal of space needed for recruiting offices, intermediate commands, and main stations of the Military Services" (DOD, 2005b). However, there are no DOD issuances directing the methods for how the respective services recruit military personnel.

5. The Military Human Resource Model

The framework for the military human resource model is set by U.S. law. Soon after World War II, Congress passed the Officer Personnel Act (OPA) of 1947 (Officer Personnel Act [OPA], 1947). This applied the Navy's "up or out" promotion system to officers in all of the services and established promotion boards based on commissioning dates. To complement the culling of the ranks established by OPA, the Officer Grade Limitation Act (OGLA) of 1954 set ratios for field grade officers to enlisted personnel (Officer Grade Limitation Act [OGLA], 1954). Contraction and expansion of military forces between and during conflicts continued to have negative effects on the Army's ability to recruit and manage its officer population. In 1980, Congress combined OPA and OGLA with other measures into the Defense Officer Personnel Management Act (DOPMA) (Defense Officer Personnel Management Act [DOPMA], 1980). DOPMA established the Army's current officer recruitment, management, and retention system. RAND published an assessment of DOPMA in 1993 (Rostker et al., 1993). Since its passage in 1980, DOPMA has been analyzed and critiqued to mixed reviews.

The transition from a conscripted force consisting of draftees to an all-volunteer force (AVF) necessitated the adoption of both "hard" and "soft" HRM constructs. "The Nixon administration created the All-Volunteer Force in 1973, in the final days of the Vietnam War.3 During the 15 years that followed, the Department of Defense built AVF 1.0, a force optimized to fight short wars with overwhelming force, and to conduct the occasional "operation other than war" (Carter, Kidder, Schafer & Swlck, 2017). DOD was now in competition with the civilian sector for labor, especially highly specialized and technical fields. The second iteration, AVF 2.0 evolved from the downsizing after the end of the Cold War and the first Gulf War (Carter, Kidder, Schafer & Swlck, 2017). AVF 2.0 went to war after the events of 9/11. The lessons learned from Iraq and Afghanistan informed the changes in AVF 3.0. This force integrated civilian, contractor, and interagency personnel to provide requisite capabilities not present in the active duty force at desired levels or not at all (Carter, Kidder, Schafer & Swlck, 2017).

Competition with civilian employers centered on compensation (Carter, Kidder, Schafer & Swlck, 2017). This increased the cost per Soldier, especially for critical specialties such as pilots, medical professionals, and information technology. DOD focused on incentive pays and comparisons of benefits to recruit and attract personnel (Hansen & Nataraj, 2011). Simultaneously, the civil military divide began to emerge in the 1990s. This was the "first peacetime All-Volunteer Force in U.S. history" (Carter, Kidder, Schafer & Swlck, 2017). The contraction and expansion of the AVF caused a general upward trend in the quality of recruits, but this masked several quality problems that have begun to manifest with varying degrees of severity (Carter, Kidder, Schafer & Swlck, 2017). One such problem with the current AVF according to the working paper, "AVF 4.0: The Future of the All-Volunteer Force," is rigidity (Carter, Kidder, Schafer & Swlck, 2017). "One particular area where such rigidity is causing immense talent management problems is the cyber field, where traditional hierarchical career paths and team management impedes the best practices in the technology sector. This not only impedes productivity within the cyber military occupational specialty but also precludes competing for the best talent in the field" (Carter, Kidder, Schafer & Swlck, 2017). The Air Force has a similar issue with pilots. System rigidity hampers innovation for incentives and bonuses. Intentional "rigidity intended to make personnel interchangeable and replaceable is having the opposite effect on highly skilled service members" (Carter, Kidder, Schafer & Swlck, 2017).

6. The Army Human Resource Model

From the Army's perspective, "HRM is a series of integrated decisions about the employment relationship that influences the effectiveness of employees and organizations" (DA, 2015a). The Military HRM (MHRM) consists of eight life cycle functions: personnel structure, acquisition, distribution, development, deployment, compensation, sustainment, and transition (Department of the Army [DA], 2015a). Recruitment falls under acquisition. Much of the language for MHRM borrows from both “hard” and “soft” military constructs. For example, special pay programs exist due to competition with both public and private sectors for matching skill sets. However, because the Army is not a for-profit endeavor, an emphasis on fiscal stewardship permeates the MHRM chapter of “How the Army Runs.”

“The Personnel Management Authorization Document (PMAD) is the authoritative source for officer requirements” (DA, 2015a). Army officers are procured or recruited from the following sources: Officer Candidate School (OCS), Reserve Officer Training Corps (ROTC), and the United States Military Academy (USMA). The aforementioned sources are for acquisition of entry level officers recruited externally. Policies and procedures for officers recruited from within the Army, more commonly known as a branch transfer, is covered under AR 614–100 “Officer Assignment Policies, Details, and Transfers” (Department of the Army, 2006). There are two types of branch transfers, voluntary and involuntary. The respective Army branches are responsible for internal recruitment to support voluntary transfers. The Voluntary Transfer Incentive Panel (VTIP) is the most notable transfer program. VTIP is a collection of established transfer processes tailored to the strategic needs of the Army. It is published as a military personnel (MILPER) message with specific instructions on the affected branches, eligibility criteria, and timelines. “The APT Program is a testing system operation encompassing standardized tests to determine eligibility for specialized training and to support the Army’s personnel selection and classification process including language proficiency testing” (DA, 2015b). Army G-1 is responsible for developing the policy for the use of tests. However, Army Human Resources Command (HRC), is responsible for the development of tests “necessary for effective personnel management” (DA, 2015b). The Armed Services Vocational Aptitude Battery (ASVAB) test is the primary tool to support personnel classification (DA, 2015b).

7. Specialty Recruitment in the Army

The special branches of the Army are Judge Advocate General Corps (JAGC), medical branches (which consists of six medical corps), Chaplain Corps, and Special Forces (DA, 2015a). U.S. Army Recruiting Command (USAREC) is responsible for recruiting most medical officers and Chaplains at the entry level (DA, 2015a). JAGC and Special Forces are responsible for recruitment of their respective commissioned officers. While Aviation is not a special branch, the personnel recruitment and evaluation process is analogous to the aforementioned special branches (DA, 2005). Internal recruitment for the special branches utilizes voluntary branch transfer mechanisms outlined in AR 614–100 (DA, 2006).

USAREC takes a tactical and operational approach to recruiting. (DA, 2014e). The organization utilizes the Military Decision Making Process (MDMP) to plan and execute recruiting operations. Tasks developed through either the Army Design Method or MDMP are grouped into eight categories, also known as the eight recruiting functions (DA, 2014e). Mission command, intelligence, prospecting, interviewing, processing, leading future Soldiers, training and leader development, and sustaining operations, comprise the eight recruiting functions. (USAREC, May 2014). The lack of threats in the recruiting environment led to a change in one of the operational variables in the planning process. “Political” considerations become “policies” in recruiting operations. Figure 6 depicts the eight recruiting functions.

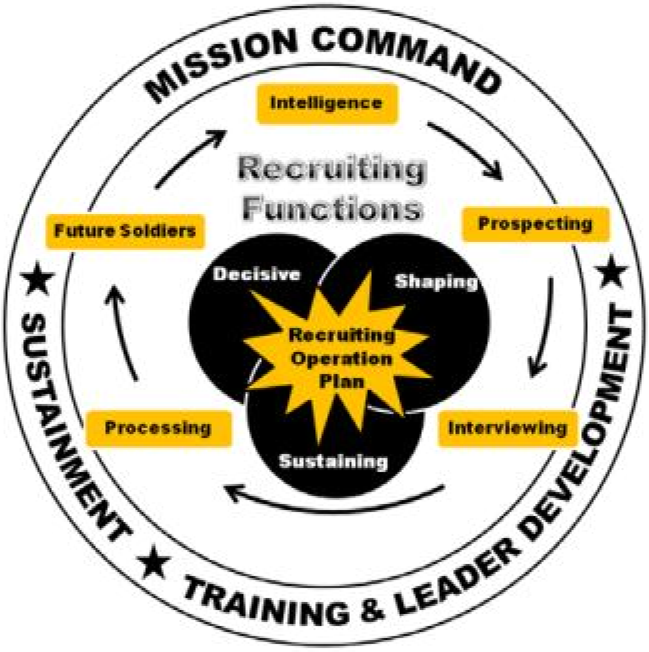


Figure 6. USAREC Recruiting Functions

Army Training and Doctrine Command (TRADOC), of which USAREC is a subordinate, is the major command overall responsible for talent acquisition. In total, 14 military organizations support and sustain recruiting functions. Of note are two marketing organizations, the Army Marketing Research Group (AMRG) and the Joint Advertising, Market Research, and Studies (JAMRS). While both entities are primarily concerned with branding for the Army and DOD, they also conduct research on external accessions (AMRG, 2017). Research conducted by both organizations assists USAREC with intelligence preparation for the various recruitment environments it faces.

Operational requirements ultimately come from two sources: operational needs from units in the field, and capability requirements to support national defense and service level strategies. (USAREC, May 2014). Unit requirements are collected by U.S. Army Forces Command (FORSCOM) and presented to TRADOC for execution. USAREC, through MDMP and the targeting process, develops a plan to acquire talent (Department of the Army, 2014f). In the case of specialty recruiting, recruits undergo physical and mental aptitude testing to determine suitability. For occupations with civilian equivalency, such as medical professionals, the Army focuses more on indoctrination during the recruitment process. A significant level of trust is placed on the credentialing institutions to ensure personnel possess the requisite skills. In the case of pilots and special forces, specific physical and aptitude testing is required due to the unique environments in which those personnel operate. The Army Flight Aptitude Selection Test (FAST) is designed to measure aptitudes specific to Army helicopter flight training (Wiener, 2005). Army Special Forces administer the Wonderlic test and other standardized cognitive tests to measure intelligence and problem solving ability (Beal, 2010). The owning Army branch is responsible for the development of occupation specific tests and lists of required credentials, with support from the aforementioned organizations. Significant research and numerous trials are conducted to ensure aptitude tests accurately predict whether prospective recruits possess the requisite skills to provide the desired capability.

C. THE RECRUITMENT OF CYBER OPERATIONS OFFICERS (17A)

1. DOD Cyber Workforce Strategy

In 2013 the DOD published the Cyberspace Workforce Strategy to transform its cyberspace workforce of military and civilian personnel. This strategy identified six strategic focus areas: 1) "Establish a cohesive set of DOD-wide cyberspace workforce management issuances;" 2) "Employ a multi-dimensional approach to recruiting;" 3) "Institutionalize continuous learning with greater focus on evaluating the maturity of skills;" 4) "Retain qualified personnel;" 5) "Expand threat knowledge;" and 6) "Understand crisis and surge requirements and options" (DOD, 2013). Strategic goal number two is particularly relevant to this research and in evaluating the effectiveness of the Army's recruitment of Cyber Operations Officers. In order to operate a multi-dimensional recruitment approach, it is essential to develop innovative methods for recruitment, including aptitude assessments, transition opportunities and development of a talent pipeline through partnerships with other government agencies (DOD, 2013). This strategy goes on to outline the critical elements for achieving this goal. One of these is assessing aptitude as well as qualifications, "The [DOD] must develop methods to assess aptitude (critical thinking and problem-solving ability) as a tool for recruitment in addition to using traditional knowledge-based qualifications for both military and civilian positions" (DOD, 2013). This strategy also finds that the creation of transition opportunities between and within military and civilian service is a critical element for achieving this goal, stating, "the Department must also develop ways to realign and transition its current workforce by recruiting them into diverse cyberspace positions" (DOD, 2013). Lastly, developing "awareness of the unique cyberspace workforce opportunities" at DOD is characterized as a critical element to achieving the goal of employing a multi-dimensional approach to recruiting (DOD, 2013). This element suggests that, "the opportunity to work in these unique mission areas in the defense of our nation will attract candidates as they see the benefits, opportunities, and challenges offered by a DOD cyberspace career" (DOD, 2013).

2. Critical Element #1: Assessing Cyber Aptitude

The Army, through the newly established Army Cyber Institute (ACI), acknowledged that the traditional military approach for filling personnel requirements is not suitable for the recruitment of cyberspace forces (Morris & Waage, 2015). Morris and Waage (2015) identify challenges in recruiting the right people for jobs in the cyber arena stating, "There is some agreement that developed cognitive problem-solving is a desired trait for cyber personnel, but there is much argument on how to measure if a candidate has it. The traditional testing method for military accessions does not properly test for desired cyber traits" (Morris & Waage, 2015). This conforms with the DOD cyber workforce strategy critical element of assessing aptitude as well as qualifications.

a. The Challenge of Cyber Aptitude Testing

While it is clearly outlined that aptitude testing is critical to the DOD Cyber Workforce Strategy and inherently the Army's recruitment of Cyber Operations Officers, Morris and Waage (2015) highlight that the issue with this type of testing is the difficulty in establishing metrics to effectively measure cyber aptitude in a potential candidate. Assessing cyber aptitude is a challenge that extends far beyond the boundaries of the DOD, however, the DOD is uniquely fettered by this due to its traditional approach to aptitude testing. Campbell et al. (2015) identify the overarching challenge more succinctly as, "determining what traits, other than existing knowledge, contribute to success in cybersecurity-related tasks" (Campbell et al., 2015). They go on to identify that characterizing what jobs are cybersecurity jobs and how those roles fit together is a key part in understanding how to determine these traits for measuring cyber aptitude (Campbell et al., 2015). Saner et al. (2016) provide some additional context, citing "perhaps the biggest challenge in testing aptitude for cyber is to isolate a concise characterization of what jobs and tasks fall within its field" (Saner et al., 2016). The National Initiative for Cyber Education (NICE) established a framework for work roles/ jobs in the field of Cyber Operations that included defining work roles in 31 cybersecurity specialty areas, grouped in seven categories with knowledge, skills and abilities (KSAs) required to perform each of them (Saner et al., 2016).

While researchers have found this framework to be useful in categorizing major job tasks, they found a lack of granularity in them that would allow them to map these work roles to cognitive processes which would be used to assess cyber aptitude (Saner et al., 2016). The ACI research on cyber aptitude assessment conducted by the Morris and Waage (2015) introduced and provided a review of three currently available testing instruments that could be used to assist with this assessment. The three testing instruments that were described were: The Cyber Aptitude and Talent Assessment (CATA), the Armed Services Vocational Aptitude Battery—Cyber Test (ASVAB-CT), and the SANS—Cyber Talent Enhanced (CTE). Each of these testing instruments described by Morris and Waage (2015) offer its own approach to assessing aptitude with its own respective metrics for predictive performance.

b. Options for Assessing Cyber Aptitude

(1) Cyber Aptitude and Talent Assessment

The CATA model of cybersecurity, created by the University of Maryland Center for Advanced Study of Language (CASL), consists of pairing cybersecurity jobs to the two portions of their cybersecurity performance model: "critical thinking and measurement of constructs" (Morris & Waage, 2015, p. 6). CATA uses two dimensions to populate cybersecurity jobs in relation to each other on an X-Y axis; X-axis = real-time/exhaustive operations and Y-axis = initiating/responding operations, as illustrated in Figure 7 (Saner et al., 2016). The intersection of these two dimensions creates a quad-chart that corresponds to the four key classes of cyber network operations defined by CASL (2015) as attack, defend, development and exploitation operations. CASL (2015) proposed that this model of cybersecurity performance/aptitude assessment was distinct from others because it contained both a critical thinking component and a job-specific component. This, they argued, would provide supervisors with information about applicants that would allow them to identify the potential they had to perform cybersecurity job roles (Center for Advanced Study of Language [CASL], 2015).

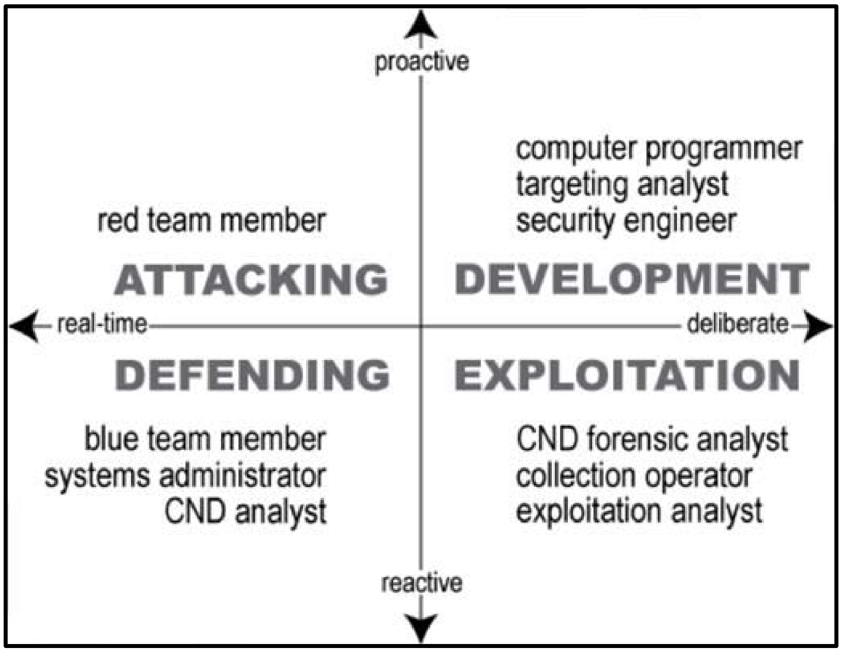


Figure 7. Dimensions of the CATA Framework. Source: Saner et al. (2016).

(2) ASVAB—Cyber Test

In 2005, the Office of the Assistant Secretary of Defense requested that the Defense Manpower Data Center (DMDC) initiate a review of the ASVAB (Trippe et al., 2014). The review resulted in 22 recommendations grouped into five areas, one being ‘content changes’ (Trippe et al., 2014). One of the content changes was information/

communications technology literacy (ICTL), which eventually morphed into ‘Cyber Test’ (CT), which the Air Force took the lead in developing (Trippe et al., 2014). To develop this testing model the Air Force came up with a taxonomy of KSAs required for successful performance in cyber/IT occupations, that consisted of 79 specific knowledge statements organized into four broad areas: networking and telecommunications, computer operations, security and compliance, and software programming and web design (Trippe et al., 2014). The Air Force conducted validity tests that measured if the performance on the aptitude test could predict performance at a technical training school and found that CT scores were better predictors than other composites used to qualify military applicants (Trippe et al., 2014). According to Morris and Waage (2015), the ASVAB-CT is more of a supplemental for the traditional military ASVAB to gauge interest, motivation and skill, a technique already used by the military to identify individuals with unique skills in other military occupational specialties (MOS). This cyber aptitude testing instrument was described as, “a cognitive measure designed as an ASVAB technical subset to predict training performance in entry-level cyber-related military occupation” (Morris & Waage, 2015).

(3) SANS—Cyber Talent Enhanced (CTE)

Morris and Waage (2015), identified the CTE as a “combined aptitude/skills exam from the SANS organization.” The SANS website states that this combined aptitude/ skills exam assesses six content areas: Information security aptitude, networking concept domain, defense in depth domain, Internet security technologies domain, communications security domain and operating systems security domain (SANS, 2017). The Army established a pilot program to use the CTE—SANS for cyber aptitude testing for enlisted members in 2013 and 2014, where approximately 60 Army personnel took the exam resulting in positive correlation results with performance of cyber related skills (Morris & Waage, 2015). In an article from NextGov.com Ballenstedt (2013) writes that CTE-SANS, “allows organizations to send assessment links directly to candidates. Once completed, the results are sent immediately back to the hiring or recruiting manager, who can review the results” (nextgov.com, 2017).

Based on the DOD Cyberspace Workforce Strategy and the available testing instruments that could be used to measure Cyber aptitude, Morris and Waage (2015) recommended the Army develop a Cyber Talent Targeting Methodology that used a modified version of the same targeting method for ‘high value individuals (HVIs)’: Find, Fix, Finish, Exploit, Steady-state and Assess (F3ESA) (Morris & Waage, 2015).

3. Critical Element #2: Transition Opportunities

The DOD Cyber Workforce Strategy lays the foundation for which the Army built its recruitment of Cyber Operations Officers on and identifies some of the resources available for its facilitation. In line with the DOD cyber workforce strategy to employ a multi-dimensional approach to recruiting cyber personnel by creating transition opportunities within the military, the primary Army recruitment strategy for the Cyber Operations Officer, was the Voluntary Transfer Incentive Program (VTIP). According to the Military Personnel (MILPER) Message 14–298: Initial 17A Cyber Branch VTIP, published in October 2014, there were 11 criteria established for applicants. The highlights of these criteria were: 1) the ability to obtain and maintain a top secret (TS) security clearance and sensitive compartmentalized information (SCI) caveat; 2) ability to obtain and maintain a counterintelligence (CI) polygraph and NSA access; 3) preferable minimum degree requirement of Bachelor of Science (BS) or higher degree in electrical engineering, computer science, computer engineering, information technology, information systems, information assurance/cyber security, or mathematics with a minimum of 6 credit hours of structured programming (Department of the Army, 2014).

4. Critical Element #3: Advertising DOD Cyberspace Workforce Opportunities

The last critical element (see section C.1) of the DOD Cyberspace Workforce Strategy goal of employing a “multi-dimensional approach to recruiting” is “developing awareness of the unique cyberspace workforce opportunities at DOD” (DOD, 2013, p. 6). This concept is addressed in Guest’s (1987) HRM model, where he talks about the quality of work dimension and identifies the value of an organization’s public image in conjunction with quality of staff and quality of performance (Guest, 1987). In addition to addressing the challenge of selling the benefits of working in the cyber community for DOD, this element infers the importance and reciprocal relationship of finding the right talent to do so. Morris and Waage touch on this slightly with their F3ESA targeting methodology where they suggest that the Army locate cyber talent by observing their routines in order to determine the places they typically gravitate to (Morris & Waage, 2015).

5. Army Recruitment of Cyber Operations Officers

With the DOD Cyber Workforce Strategy in place and three critical elements being identified for the achievement of the strategic goal of employing a multi-dimensional approach to recruiting, this is what the Army did to recruit Cyber Operations Officers. As outlined in the Chapter I, in December 2014 the Army started the recruitment process for the officer requirement for CF17 with a Voluntary Transfer Incentive Panel (VTIP) targeted at the existing Army Officer Corps and a simultaneous in-service accessions campaign at West Point and ROTC programs targeted at future Army officers (Human Resources Command-Cyber [HRC–Cyber], 2016). The Army Cyber School—established on August 4, 2013—created a single set of criteria for the consideration of applicants for selection/transition into the Cyber Branch. These criteria were separated by rank, performance and skills/experience and evaluated as either highly qualified, qualified or not qualified (Army Cyber School [ACS], 2017).

Despite the criticality identified by the DOD Cyberspace Workforce Strategy for aptitude testing and the acknowledgement from the ACI that the traditional military approach would not suffice, the Army's initial recruitment of Cyber Operations Officers did not use any formal aptitude testing to select the first 17A cohort. According to MILPER message 14–298, the only application requirements were: a completed and signed DA Form 4187 (Personnel Action); a memorandum for record (MFR) stating the reason for applying; school transcripts; proof of certifications; Curriculum Vitae (CV) and/or Resume with "any pertinent cyber/IT related background"; letters of recommendation and; Officer Evaluation Reports (OER) (DOD, 2014). The Cyber Center of Excellence (CCoE) reported that after the initial VTIP, a cyber questionnaire created by ACI and the Cyber School was added as a requirement to the application process.

The duties and responsibilities of a Cyber Operations Officer are outlined in the update to DA PAM 600–3, which is still in draft form. “Cyber operations officers conduct offensive cyberspace operations (OCO) by projecting power through the application of force in and through cyberspace to target enemy and hostile adversary activities and capabilities” and/or, “conduct defensive cyberspace operations (DCO) by protecting data, networks, net-centric capabilities, and other designated systems through detection, identification, and response actions to attacks against friendly networks” (Department of the Army, 2014). In addition, this draft update identifies some of the characteristics/attributes required of a Cyber operations officer. These attributes include: “possessing a terrain sense,” “passion for precision,” “tenacity” and “audacity.” The more distinguishable attributes were identified as: a well-developed understanding of cyber operations, advanced computer literacy and ability to command cyber operations assets and formations (Department of Army, 2014).

In reference to recruiting Cyber Operations Officers, Arnold, Harrison and Conti suggest that currently, “leaders capable of serving in the cyber realm are developed in an ad hoc manner; in most cases the development occurs despite the current system, not because of it” (Arnold, Harrison & Conti, 2013). Harris and Morris identify the fundamental issue behind the flawed approach to recruiting cyber talent as a “lack of institutional understanding regarding cyberspace as a warfighting domain” in addition to the competitive talent search and inherent incentives required to attract talent (Harris & Morris, 2016). There is a lack of academic research addressing the effectiveness of the Army’s HRM for recruiting Cyber Operations Officers compared to proven HRM practices in nonmilitary recruitment of similar occupational requirements. In the next chapter we describe how we approached addressing this gap.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY

The purpose of this chapter is to explain the methodology used to collect and analyze our data. In order to evaluate the HRM used by the U.S. Army to recruit Cyber Operations Officers we applied a mixed method approach with both quantitative and qualitative techniques, which will be detailed later in this chapter. As highlighted by Arthur and Boyles (2007), to assess the effectiveness of an organization's HRM model researchers should focus on the Human Resource (HR) systems of that organization. Therefore, the HR systems we observe to evaluate the Army's HRM for the recruitment of 17As are "HR programs and practices," as these components each address the recruitment and selection processes. The data sources for these systems include:

- the Person-Event Data Environment (PDE) database;
- an online survey of current Cyber Operations Officers (17As);
- the Army Human Resource Command Cyber Branch proponent (HRC–Cyber);
- the Army Cyber Center of Excellence (CCoE);
- Army Cyber (ARCYBER);
- Department of Homeland Security (DHS);
- Facebook;
- Google; and
- existing relevant literature on the recruitment of Cyber Security Professionals.

The data that was collected from these sources included:

- details of the Army recruitment strategy for 17As
- MTOE requirements for the Cyber Mission Force
- selection criteria for the initial cohort of Cyber Operations Officers
- key attributes/characteristics of selected 17As

- duties and responsibilities expected of 17As
- best practices/industry standards and a host of other significant data points from case studies and existing literature

This chapter will discuss each of these data sources, provide an overview of the data collected from them and address the rationale for their use in addressing our research questions. Lastly, we present the parameters used for the comparative analysis between Army recruiting of Cyber Operations Officers and government and non-government organizations, establishing the baseline for our comparison including both the limitations and value of the comparison.

A. RESEARCH GOALS

We answer our research questions by identifying the HRM model used by the U.S. Army to recruit Cyber Operations Officers and evaluating its effectiveness.

1. Quantitative Approach

We first determined how closely the Army's targeted population, attributes and numbers identified in its recruitment strategy match the actual quantitative data collected from the PDE database and from our survey of current 17As. The data needed to identify the recruitment strategy were collected from Army institutions to include; the HRC–Cyber, CCoE and ARCYBER. This research addresses the Army's target variables to include:

- the target population—whom/where to recruit 17As from
- the target attributes—key desired abilities/characteristics
- the target manning—how many 17As to recruit

These are what we refer to as "should hit" data. To measure how closely these target variables match the actual current 17A population, which we refer to as "did hit" data, quantitative data sets from the PDE database were used, and we designed and conducted a survey of the entire current population of 17As. Each of these data sets provided different data points for the target variables and subsets of these variables which were used to measure “should hit” versus “did hit” data. By applying these data sets and elements of the recruitment strategy, this research identifies measures of performance (MOP) to understand how successful the Army has been at conducting its strategy of 17A recruitment and measures of effectiveness (MOE) to understand the effect of the strategy. In the U.S. military, MOPs are one of the indicators of progress or regression in an assessment of an operation. Its purpose is to evaluate internal actions associated with the assessing of the completion of tasks and to answer the question, “Are we accomplishing tasks to standard?” (Joint Publication [JP] 3–0, 2017, p. II-12). The other indicator, as highlighted in JP 3–0 (2011), is MOEs, which are designed to “assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect” and to answer the question “Are we creating the effect(s) or conditions in the OE [Operational Environment] that we desire?” (JP 3–0, 2011, p. II-12). For our research, with regard to MOPs and MOEs, the operation being assessed is the recruitment of 17As, the tasks are those outlined in the recruitment strategy and target goals. The standard is a metric based achievement rate and the OE is the Cyber Branch.

With regard to MOEs, ideally the “effect” would be a highly qualified population of 17As validated by objective evaluations of their performance, technical expertise, potential and impact. However, due to the recent creation of the Cyber Branch, selection of 17As, and other research constraints, objective measures to evaluate the current population of selected 17As are not available. Instead we establish proxy MOEs based on frameworks discovered in our literature review and our personal operational experiences. Our MOEs will be in the subjective categories of job satisfaction, assessment of the recruitment process and motivation for becoming a 17A. Specific questions in our survey address these categories. To validate and assess these MOEs we partnered with TRADOC Analysis Center (TRAC)–Monterey to analyze our survey results. The mission of TRAC–Monterey is to “perform relevant and credible exploratory and applied research to support the TRAC mission” (TRADOC, 2010). TRAC–Monterey helped us to conduct both exploratory and factor analysis of our survey data to establish correlations between variables and identify the optimal number of factors, through factor analysis, to use in a regression tree model for the analysis of our data. According to Yong and Pearce (2013, p. 79), the purpose of factor analysis is to "summarize data so that relationships and patterns can be easily interpreted and understood." Factor analysis will show to what degree the attributes identified in the Army's recruitment strategy are linked to our designated proxy MOEs.

2. Qualitative Approach

Upon evaluation of the Army's initial recruitment of 17As from 2014–15, we evaluate whether the Army's strategy is optimal for its goals. We assess how the Army's recruitment strategy and target goals leverage best practices and industry standards of selected other government and non-government entities, by studying multiple qualitative data sources:

- open-ended subjective questions from the 17A survey
- observations from CCoE, ARCYBER, ACI and Cyber Branch professionals
- relevant published literature; and
- data provided by DHS and Facebook

These sources offer insight into whether the right attributes were targeted for recruitment of 17As, and whether their skill sets were appropriately assessed for selection. Of note, we conducted sentiment analysis of the open ended questions from the 17A survey. The subjective responses were categorized as "recruitment related" or "selection related" and with assistance from TRAC–Monterey we analyzed these observations to add context to our analysis. Using the remaining data sources, we established a baseline for comparison, taking into account Army regulations that place restrictions on recruitment and selection practices. Once these restrictions were considered, a list of comparable elements of the recruitment and selection processes and targeted goals was created. This part of the research adds some context beyond the quantitative measures to understand the logic behind the targeted attributes and to gain a more holistic view of the effectiveness of the

Army's recruitment of the 17A in comparison to selected other organizations. Measures used for evaluating effectiveness in this component of recruiting 17As mostly identify key similarities and differences between the Army's recruitment process, best practices and industry standards, as identified by relevant literature and data collected from selected other government and non-government organizations.

B. DATA COLLECTION

This research applies a mixed method approach with both quantitative and qualitative data. Data collection and analysis focus on the PDE database, the survey of the current population of 17As, and data from the Army institutions that collect and record quantitative data on Cyber Operations Officers and the Cyber Branch. The data supports measuring how successful the Army has been at achieving its targeted recruitment goals, and the effectiveness of these goals and identifies relevant relationships between variables. The quantitative data collected also facilitate the construction of statistical models to predict 17A job satisfaction, assessment of the recruitment process and motivation for becoming a 17A. The primary purpose for collecting data from PDE is to compare the survey data to the population of 17As. Demographic proportions for gender, age, rank, and education level is compared with the survey data. This is done to determine the level of confidence with which the survey data is representative of the population of 17As. The number of respondents is compared against the PDE data to determine response rates for the population as a whole and by the aforementioned demographic identifiers.

In addition to survey validation, the PDE data is compared to DOD and Army reported statistics on gender, age, race, and rank. These descriptive statistics help with understanding the population of Army Cyber Operations officers beyond the key desired characteristics of experience, education level, and industry credentials. This is intended to identify any significant deviations from DOD or Army proportions.

The qualitative data used in this research included the data from open-ended survey responses from current 17As, from other selected government and non-government organizations, relevant published literature and information provided by personnel at Army institutions that have participated in and have significant background information on the recruitment of Cyber Operations Officers. These data were used to heuristically assess how the Army recruitment process and targeted goals for 17As align with other selected organizations, best practices and industry standards, to understand subjective experiences and organizational processes; and to ultimately evaluate the Army's HRM effectiveness for recruiting Cyber Operations Officers.

1. PDE Data

The primary source of quantitative data collection for this research is personnel data from the PDE. "The PDE is a consolidated data repository that contains unclassified but sensitive manpower, training, financial, health, and medical records covering U.S. Army personnel (Active Duty, Reserve, and National Guard), civilian contractors, and military dependents" (PDE, 2017). Data collected from PDE is the official Army record of Cyber Operations Officers in formations at the time of capture. This data represents the baseline or control group for comparison with other quantitative and qualitative data collected. Administrative and personnel data on the current population of officers that possess the 17A Cyber Operations Officer military occupational specialty (MOS) was requested from the Army's master personnel database. To provide a comprehensive picture of the population from the Army's perspective, the data set is subjected to a variety of descriptive statistical techniques. A request for the data was submitted on February 8, 2017. PDE provided administrative and personnel data records for 373 17As in a virtual environment on June 13, 2017.

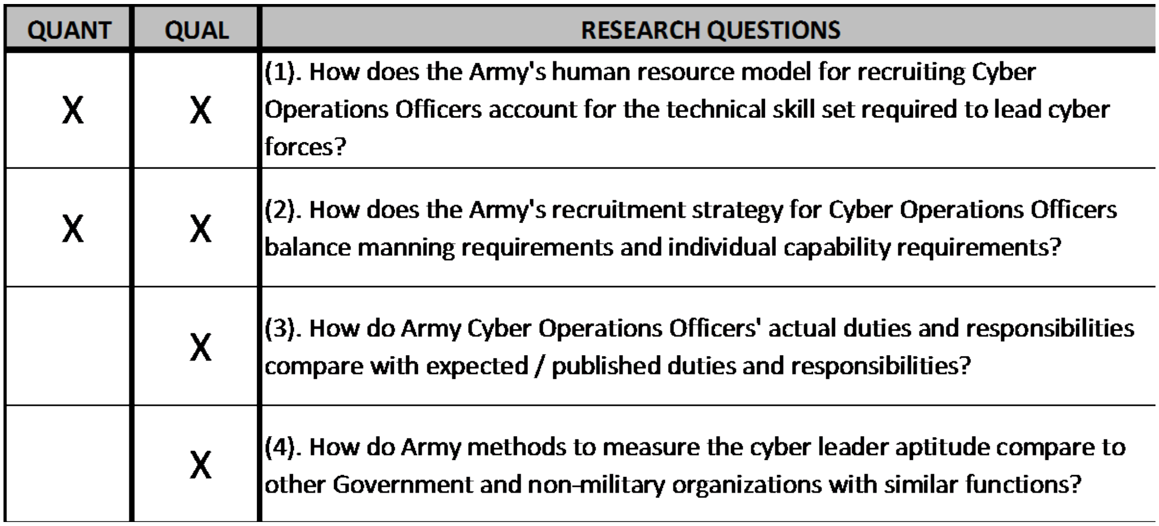
While the data collected from the Army master personnel record within PDE contains most of the variables on the 17A population, it does not paint the complete picture. Data on civilian certifications and some civilian education information (undergraduate and graduate degree type, and majors) were not available via the master personnel record at the time of the request. We detected a conflict regarding the total number of 17As between Cyber Branch and what is reported in the master personnel record, 393 and 373 respectively. That is a difference of 20 officers. The amount of time required for PDE to fulfill each data request rendered subsequent requests infeasible for reconciliation. The difference between the official record, Army Cyber Branch reports, and the survey discussed later in this chapter, has the potential to impact correlations and inferences for specific officer rank populations. For our purposes we use 373 for the number of 17As reported by the Army because it is sourced from the Army Master Personnel database. This depends on whether the distribution of the 56 Officers is spread across all ranks in proportion to their respective density. Finally, the data within PDE relies on the affected Officer population for accuracy. The data used for the purposes of this research is a snapshot in time and does not reflect changes made due to promotion board results, permanent change of station (PCS), or attainment of post graduate education and training.

2. Cyber Operations Survey Data

To evaluate the Army's recruitment strategy we determined that an appropriate technique would be to design and implement a survey to the entire population of 17As. Following Dillman et al. (2009), we generated a web-based survey and created the questions using a tailored design method targeted towards the current 17A population. The survey questions included several focus areas: demographics, educational/ professional background, current duty position/assignment, job satisfaction, motivations, assessment of the recruitment process, ranking key attributes and open ended questions on the overall process.

We conducted a pilot test of the survey ten days prior to full deployment to work out any issues. Prior to the survey invitation being sent, we sent a pre-survey message detailing the purpose of the survey and the timeline for its implementation. Additionally, we sent two reminders after the initial survey invitation was sent to ensure maximum participation. The survey was opened on December 17, 2016 and the invitation to participate was sent to 363 current Cyber Operations Officers, as identified by the HRC–Cyber. The survey closed on February 17, 2017 and of the 363 invitations, there were 236 respondents, 192 of whom completed the full survey, with a 52% response rate. The survey was used to quantify data points to assist in answering the research questions listed in Table 2.

Table 2. Research Questions Addressed by 17A Survey Data.

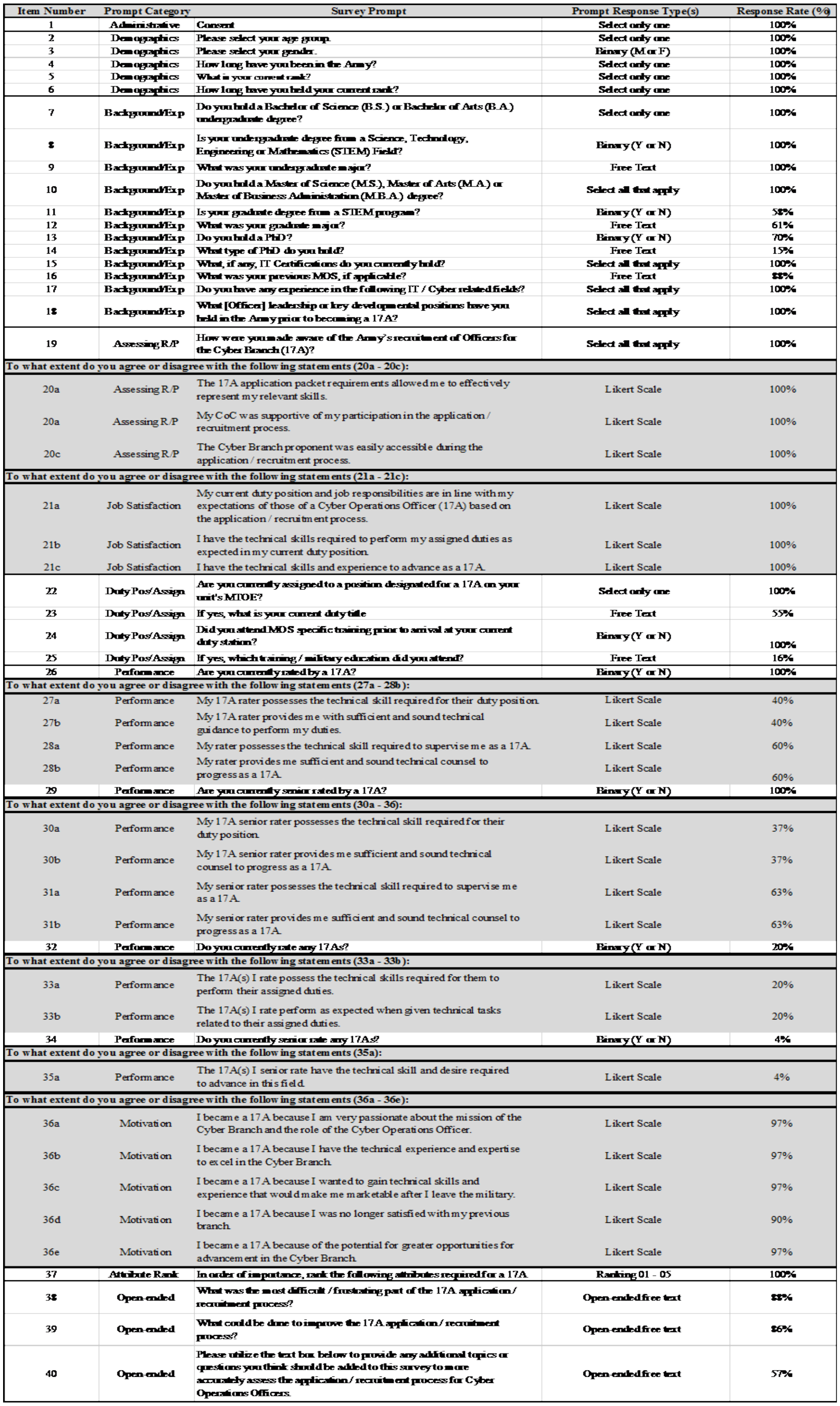


QUANT	QUAL	RESEARCH QUESTIONS
X	X	(1). How does the Army's human resource model for recruiting Cyber Operations Officers account for the technical skill set required to lead cyber forces?
X	X	(2). How does the Army's recruitment strategy for Cyber Operations Officers balance manning requirements and individual capability requirements?
	X	(3). How do Army Cyber Operations Officers' actual duties and responsibilities compare with expected / published duties and responsibilities?
	X	(4). How do Army methods to measure the cyber leader aptitude compare to other Government and non-military organizations with similar functions?

The specific quantitative categories these data were used to address include: evaluation metrics for applicants, key attributes of selected 17As, utilization metrics and duties and responsibilities of current Cyber Operations Officers performing outside of those published. These data points allow us to address MOPs and state results in context of comparative analysis and understanding how successful the Army has been at conducting its 17A recruitment strategy. Additionally, our factor analysis of this data allows us to address MOEs and evaluate the effect of the Army’s 17A recruitment strategy. The qualitative data allowed us to conduct content analysis of open ended subjective responses provided by survey participants to assist in comparing the Army recruitment processes with other organizations, best practices and industry standards.

Survey participants were asked to respond to a total of 40 prompts including the statement of consent and three open-ended questions. Table 3 displays the survey category, prompt, prompt response types and response rates (see also Supplemental, Appendix A).

Table 3. Survey Questionnaire Prompts and Response Rates



Item Number	Prompt Category	Survey Prompt	Prompt Response Type(s)	Response Rate (%)
1	Administrative	Consent	Select only one	100%
2	Demographics	Please select your age group.	Select only one	100%
3	Demographics	Please select your gender.	Binary (M or F)	100%
4	Demographics	How long have you been in the Army?	Select only one	100%
5	Demographics	What is your current rank?	Select only one	100%
6	Demographics	How long have you held your current rank?	Select only one	100%
7	Background/Exp	Do you hold a Bachelor of Science (B.S.) or Bachelor of Arts (B.A.) undergraduate degree?	Select only one	100%
8	Background/Exp	Is your undergraduate degree from a Science, Technology, Engineering or Mathematics (STEM) Field?	Binary (Y or N)	100%
9	Background/Exp	What was your undergraduate major?	Free Text	100%
10	Background/Exp	Do you hold a Master of Science (M.S.), Master of Arts (M.A.) or Master of Business Administration (M.B.A.) degree?	Select all that apply	100%
11	Background/Exp	Is your graduate degree from a STEM program?	Binary (Y or N)	58%
12	Background/Exp	What was your graduate major?	Free Text	61%
13	Background/Exp	Do you hold a PhD?	Binary (Y or N)	70%
14	Background/Exp	What type of PhD do you hold?	Free Text	15%
15	Background/Exp	What, if any, IT Certifications do you currently hold?	Select all that apply	100%
16	Background/Exp	What was your previous MOS, if applicable?	Free Text	88%
17	Background/Exp	Do you have any experience in the following IT / Cyber related fields?	Select all that apply	100%
18	Background/Exp	What [Officer] leadership or key developmental positions have you held in the Army prior to becoming a 17A?	Select all that apply	100%
19	Assessing R/P	How were you made aware of the Army's recruitment of Officers for the Cyber Branch (17A)?	Select all that apply	100%
To what extent do you agree or disagree with the following statements (20a - 20c):				
20a	Assessing R/P	The 17A application packet requirements allowed me to effectively represent my relevant skills.	Likert Scale	100%
20a	Assessing R/P	My CoC was supportive of my participation in the application / recruitment process.	Likert Scale	100%
20c	Assessing R/P	The Cyber Branch proponent was easily accessible during the application / recruitment process.	Likert Scale	100%
To what extent do you agree or disagree with the following statements (21a - 21c):				
21a	Job Satisfaction	My current duty position and job responsibilities are in line with my expectations of those of a Cyber Operations Officer (17A) based on the application / recruitment process.	Likert Scale	100%
21b	Job Satisfaction	I have the technical skills required to perform my assigned duties as expected in my current duty position.	Likert Scale	100%
21c	Job Satisfaction	I have the technical skills and experience to advance as a 17A.	Likert Scale	100%
22	Duty Pos/Assign	Are you currently assigned to a position designated for a 17A on your unit's MTOE?	Select only one	100%
23	Duty Pos/Assign	If yes, what is your current duty title	Free Text	55%
24	Duty Pos/Assign	Did you attend MOS specific training prior to arrival at your current duty station?	Binary (Y or N)	100%
25	Duty Pos/Assign	If yes, which training / military education did you attend?	Free Text	16%
26	Performance	Are you currently rated by a 17A?	Binary (Y or N)	100%
To what extent do you agree or disagree with the following statements (27a - 28b):				
27a	Performance	My 17A rater possesses the technical skill required for their duty position.	Likert Scale	40%
27b	Performance	My 17A rater provides me with sufficient and sound technical guidance to perform my duties.	Likert Scale	40%
28a	Performance	My rater possesses the technical skill required to supervise me as a 17A.	Likert Scale	60%
28b	Performance	My rater provides me sufficient and sound technical counsel to progress as a 17A.	Likert Scale	60%
29	Performance	Are you currently senior rated by a 17A?	Binary (Y or N)	100%
To what extent do you agree or disagree with the following statements (30a - 36):				
30a	Performance	My 17A senior rater possesses the technical skill required for their duty position.	Likert Scale	37%
30b	Performance	My 17A senior rater provides me sufficient and sound technical counsel to progress as a 17A.	Likert Scale	37%
31a	Performance	My senior rater possesses the technical skill required to supervise me as a 17A.	Likert Scale	63%
31b	Performance	My senior rater provides me sufficient and sound technical counsel to progress as a 17A.	Likert Scale	63%
32	Performance	Do you currently rate any 17As?	Binary (Y or N)	20%
To what extent do you agree or disagree with the following statements (33a - 33b):				
33a	Performance	The 17A(s) I rate possess the technical skills required for them to perform their assigned duties.	Likert Scale	20%
33b	Performance	The 17A(s) I rate perform as expected when given technical tasks related to their assigned duties.	Likert Scale	20%
34	Performance	Do you currently senior rate any 17As?	Binary (Y or N)	4%
To what extent do you agree or disagree with the following statements (35a):				
35a	Performance	The 17A(s) I senior rate have the technical skill and desire required to advance in this field.	Likert Scale	4%
To what extent do you agree or disagree with the following statements (36a - 36e):				
36a	Motivation	I became a 17A because I am very passionate about the mission of the Cyber Branch and the role of the Cyber Operations Officer.	Likert Scale	97%
36b	Motivation	I became a 17A because I have the technical experience and expertise to excel in the Cyber Branch.	Likert Scale	97%
36c	Motivation	I became a 17A because I wanted to gain technical skills and experience that would make me marketable after I leave the military.	Likert Scale	97%
36d	Motivation	I became a 17A because I was no longer satisfied with my previous branch.	Likert Scale	90%
36e	Motivation	I became a 17A because of the potential for greater opportunities for advancement in the Cyber Branch.	Likert Scale	97%
37	Attribute Rank	In order of importance, rank the following attributes required for a 17A.	Ranking 01 - 05	100%
38	Open-ended	What was the most difficult / frustrating part of the 17A application / recruitment process?	Open-ended free text	88%
39	Open-ended	What could be done to improve the 17A application / recruitment process?	Open-ended free text	86%
40	Open-ended	Please utilize the text box below to provide any additional topics or questions you think should be added to this survey to more accurately assess the application / recruitment process for Cyber Operations Officers.	Open-ended free text	57%

3. Data Collected from Army Institutions

The primary purpose of data from Army Institutions was to observe what the Army's recruitment strategy and target goals are and how they align with the quantitative statistical data collected from both the PDE database and our survey to provide a more complete picture for analysis. To identify the strategy used by the U.S. Army to recruit Cyber Operations Officers we analyzed documents provided by the Army HRC–Cyber, CCoE and ARCYBER. These documents include:

1. Draft DA PAM 600–3 for the Cyber Operations Officer (09FEB17)
2. The Cyber Work Role Working Group Power Point Presentation (n.d.)
3. HRC Cyber Branch Dashboard (as of 03MAR17)
4. Officer VTIP Analysis Power Point Presentation (n.d.)
5. 17A VTIP MILPER Message 14–298 (08OCT14)
6. Initial Cyber VTIP Scoring Criteria (10JUN15)
7. 17A Application Packet
8. CSA Army Cyber Personnel Implementation Strategy (25SEP14)
9. Cyber Career Field Update (28MAY14)
10. Transition Panel Criteria—Internal Review (15FEB17)
11. Cyber Road Show Slide (n.d.)

a. Human Resources Command (HRC)—Cyber Data

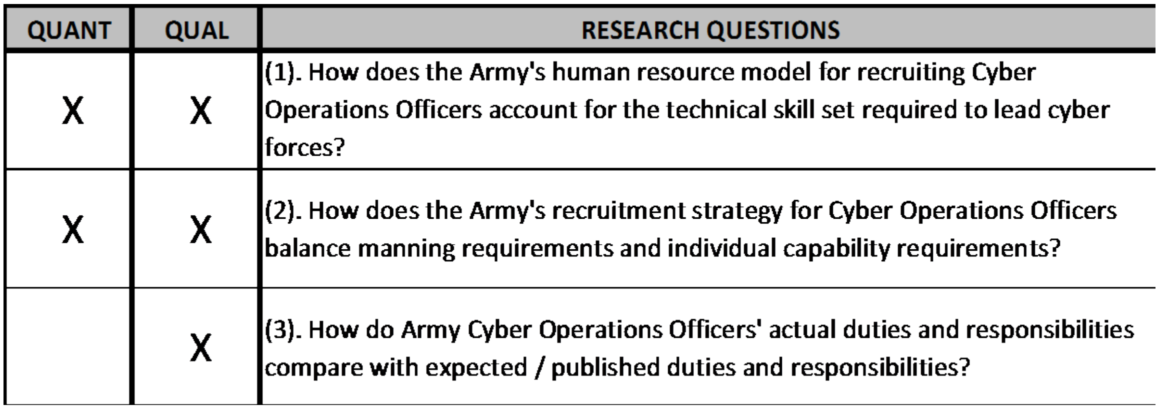
To gather some of the data contact was made with the Army HRC–Cyber. The Cyber Branch Career Manager was contacted on May 14, 2016 and the following data was requested and received:

- Human resource model for 17A recruitment (current and future)
- Recruitment goals (authorized/required/strength/priority)
- MTOE authorizations/force structure

- Duty positions/titles/descriptions
- Current or recently published MILPERs/orders/doctrine/policy for 17A

This data helped to answer three of our research questions, highlighted in Table 4.

Table 4. Research Questions Addressed by HRC–Cyber Data



QUANT	QUAL	RESEARCH QUESTIONS
X	X	(1). How does the Army's human resource model for recruiting Cyber Operations Officers account for the technical skill set required to lead cyber forces?
X	X	(2). How does the Army's recruitment strategy for Cyber Operations Officers balance manning requirements and individual capability requirements?
	X	(3). How do Army Cyber Operations Officers' actual duties and responsibilities compare with expected / published duties and responsibilities?

The specific areas these data were used to address include the following categories; the application and selection process, evaluation metrics for applicants, utilization metrics/guidance, non-standard duties and responsibilities, functions of the Cyber Operations Officer as defined by regulation, and the Army’s recruitment strategy for Cyber Operations Officers. Data were collected through coordination with key personnel at the Cyber Branch and resulted in the collection of most of the requested data with redirection to other Army institutions for additional information.

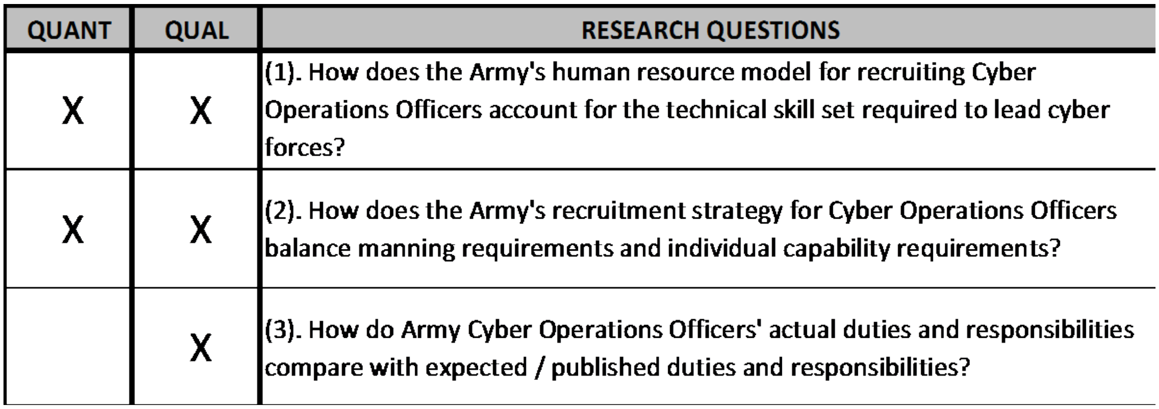
b. Army Cyber Center of Excellence (CCoE) Data

The Army CCoE was created to develop agile and adaptive Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) solutions for Cyberspace Operations (CCoE, 2014). The “P” of DOTMLPF, personnel, deals with the recruitment of Cyber Operations Officers to meet cyber capability requirements, inherently making the CCoE a vital data source for this study. We reached out to CCoE, to include the Army Cyber School, on August 1, 2016, requesting the following information:

- Updated/finalized DA-PAM for the Cyber Operations Officer (or latest edit).
- Selection criteria for Cyber Operations Officers (what does the CCoE define as essential attributes of a 17A: certs, education, experience, previous MOS, etc.).
- Board results from the initial VTIP (or a POC who could get us that information).
- CCoE involvement in HRC selection process of Cyber Operations Officers
- Training/certification requirements for selected officers.
- Percentage/number of VTIP selected officers that have attended and successfully completed the 17A qualification course.
- Percentage/number of VTIP selected officers that have attended and failed to complete the 17A qualification course.
- Percentage/number of VTIP selected officers that have not attended 17A qualification course.
- Percentage/number of assessed officers that have attended and successfully completed Cyber BOLC.
- Percentage/number of assessed officers that have attended and failed to complete Cyber BOLC.

As shown in Table 5, this data was used to answer some part of all of the research questions in this study:

Table 5. Research Questions Addressed by CCoE Data



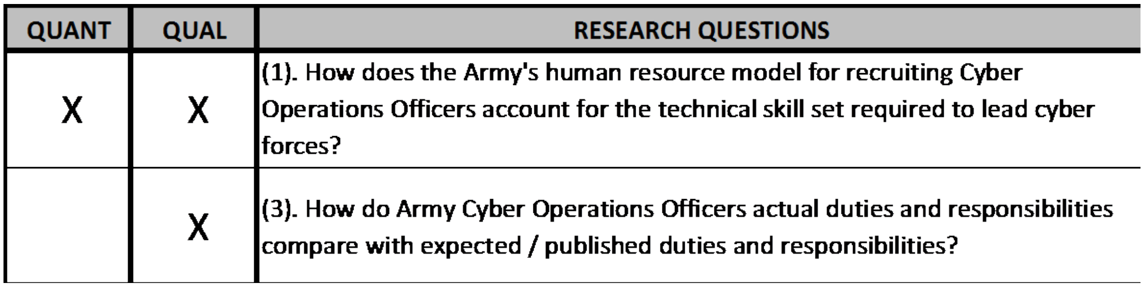
QUANT	QUAL	RESEARCH QUESTIONS
X	X	(1). How does the Army's human resource model for recruiting Cyber Operations Officers account for the technical skill set required to lead cyber forces?
X	X	(2). How does the Army's recruitment strategy for Cyber Operations Officers balance manning requirements and individual capability requirements?
	X	(3). How do Army Cyber Operations Officers' actual duties and responsibilities compare with expected / published duties and responsibilities?

The specific areas this data was used to address include the following categories; the application and selection process, evaluation metrics for applicants, utilization metrics/guidance, manning requirements/authorizations, individual capability requirements, non-standard duties and responsibilities, functions of the Cyber Operations Officer as defined by regulation, the Army’s recruitment strategy for Cyber Operations Officers, expectations of recruited 17As, training of recruited 17As, gaps in selection criteria and duty requirements, mission/makeup of the Cyber Force Structure and regulations guiding 17A recruitment. The data were collected through coordination with key personnel at the CCoE and resulted in the collection of most of the requested data.

c. Army Cyber (ARCYBER) Data

The mission of ARCYBER is to, “direct and conduct integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries” (DA, 2016). As the operational arm of the Army’s Cyber Branch, ARCYBER provides a distinct view into the real world functionality of 17As to provide context for success of targeted goals of the recruitment process and assessment of the effectiveness of those goals. Data collected from ARCYBER assisted the authors with answering the research questions listed in Table 6.

Table 6. Research Questions Addressed by ARCYBER Data



QUANT	QUAL	RESEARCH QUESTIONS
X	X	(1). How does the Army's human resource model for recruiting Cyber Operations Officers account for the technical skill set required to lead cyber forces?
	X	(3). How do Army Cyber Operations Officers actual duties and responsibilities compare with expected / published duties and responsibilities?

The specific areas this data was used to address include the following categories; functions of the Cyber Operations Officer as defined by regulation, expectations of recruited 17As, training of recruited 17As, gaps in selection criteria and duty requirements, and mission/makeup of the Cyber Force Structure.

4. Army Recruitment Strategy for Cyber Operations Officers

Based on the data collected from these Army institutions we were able to identify "should hit data" for the recruitment of Cyber Operations Officers, we analyzed the data and derived the following information:

1) U.S. Army Recruitment Strategy for Cyber Operations Officers

a. Recruitment Process

- Target population
- Target attributes
- Target manning

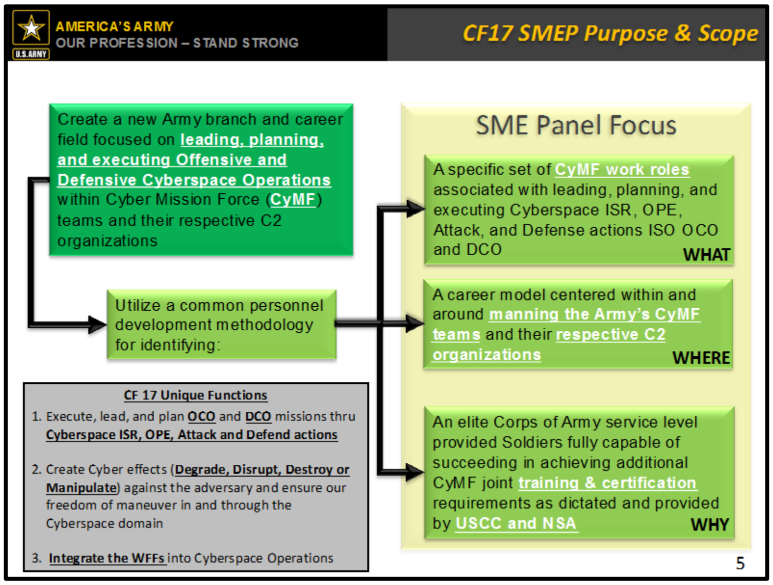
b. Selection Process

2) U.S. Army Cyber Work Roles (Cyber Operations Officer duties and responsibilities)

a. U.S. Army Recruitment Strategy for Cyber Operations Officers

In May of 2014 the Cyber Center of Excellence (CCoE) conducted a Cyber Career Field update where they discussed the personnel and training "way ahead" for the implementation of the 17-Series Career Field. In this update, the CCoE identified a 60, 90 and 120-Day phased effort that included establishing and conducting a subject matter expert (SME) panel and finalizing CMF 17 career field products. The goals for these efforts included: producing a “list of 17-Series MOS/AOC/FA and associated access, train and retain;” finalizing CF 17 MOS descriptions; creating position codes for the 17-series; identifying requirements for personnel classifications and creating a 17-Series Officer Training Course (CCoE, 2014b). While this update was heavily focused on the training portion of the “way ahead,” the beginnings of the considerations that shaped the recruitment strategy can be clearly identified. Specifically, this CCoE update identifies 30 Cyber Mission Force work roles and 13 current MOSs that could operate in those work roles at the time of the update and prior to the implementation of the 17-series career field. Only three of the 30 CMF work roles and two MOSs were identified as officer positions. This implies that, at this point, the officers’ role in the functioning of the new 17-series career field was considered minor at best, and arguably less pivotal to the overall recruitment strategy. This update outlined the strategic plan for the implementation of CF17 and introduced the specific job requirements/work roles for the CMF, while also implicitly highlighting where Cyber Operations Officers fit in (CCoE, 2014b).

In September, 2016, the CCoE conducted the CF17 SME Panel to discuss the Cyber Career Field Implementation Plan. The purpose and scope of this panel is identified in Figure 8:



AMERICA'S ARMY
OUR PROFESSION – STAND STRONG

CF17 SMEP Purpose & Scope

Create a new Army branch and career field focused on **leading, planning, and executing Offensive and Defensive Cyberspace Operations** within Cyber Mission Force (**CyMF**) teams and their respective C2 organizations

Utilize a common personnel development methodology for identifying:

CF 17 Unique Functions

1. Execute, lead, and plan **OCO** and **DCO** missions thru **Cyberspace ISR, OPE, Attack and Defend actions**
2. Create Cyber effects (**Degrade, Disrupt, Destroy or Manipulate**) against the adversary and ensure our freedom of maneuver in and through the Cyberspace domain
3. **Integrate the WFFs** into Cyberspace Operations

SME Panel Focus

A specific set of **CyMF work roles** associated with leading, planning, and executing Cyberspace ISR, OPE, Attack, and Defense actions ISO OCO and DCO **WHAT**

A career model centered within and around **manning the Army's CyMF teams** and their **respective C2 organizations** **WHERE**

An elite Corps of Army service level provided Soldiers fully capable of succeeding in achieving additional CyMF joint **training & certification** requirements as dictated and provided by **USCC and NSA** **WHY**

5

Figure 8. Career Field 17 SME Panel Purpose and Scope.
Source: CCoE (2014a).

While this panel had more of a mission focus than recruitment focus, we continue to see elements of the recruitment strategy develop as the mission/strategy becomes clarified and the work roles are better defined. This panel provided additional clarity to the work roles introduced in the Cyber Career Field Update by creating three categories to place them in: 1) Core Career Field 17; 2) Direct Support to Cyber and 3) Specialized Support to Cyber (CCoE, 2014a). This panel also discussed the recruitment process directly, proposing a "special accession panel/recruiting team" to create a pool of candidates with STEM degrees/majors, specifically in Electrical Engineering (EE), Computer Science (CS), Computer Engineering (CE), Information Technology (IT), Information Sciences (IS), Information Assurance or Math (CCoE, 2014a). They also discussed the selection process, suggesting the use of "Cyber Talent Assessment Testing" for VTIP of non-STEM talent.

(1) Recruitment Process

The overall recruitment strategy includes both the recruitment and the selection processes and before the selection of candidates can take place a pool of potential candidates has to be created. Our research examines the recruitment process used by the

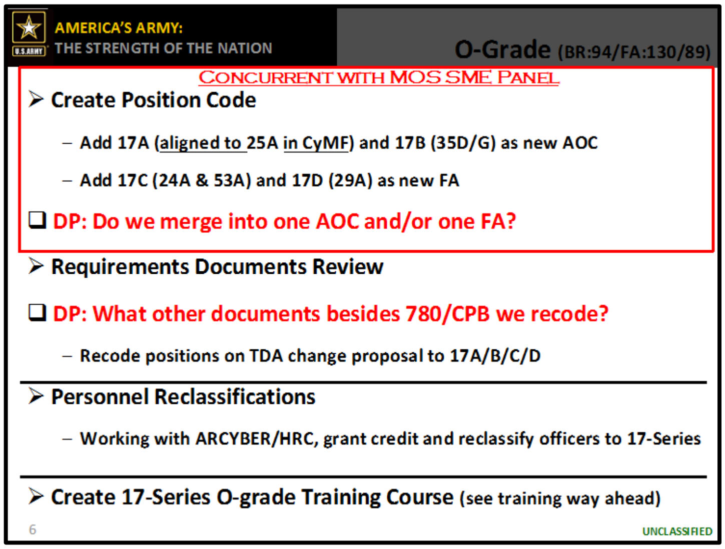
U.S. Army to create a pool of potential candidates for selection to become Cyber Operations Officer. To examine this process we analyzed the Army’s target population, target attributes and target manning for recruiting the Cyber Operations Officer.

a. Target Population

In October of 2014 MILPER message 14–298 was published Army-wide establishing the eligibility criteria for participation in the 17A Cyber Branch VTIP. The eligibility criteria were mostly standard, but also included the following qualifications:

> **J.** OFFICERS REQUESTING TRANSFER TO CYBER BRANCH MUST ADHERE TO THE FOLLOWING QUALIFICATIONS:
>
> **(3)** PREFERRED DEGREES INCLUDE AT A MINIMUM BACHELORS OF SCIENCE OR HIGHER DEGREE IN ELECTRICAL ENGINEERING, COMPUTER SCIENCE, COMPUTER ENGINEERING, INFORMATION TECHNOLOGY, INFORMATION SYSTEMS, INFORMATION ASSURANCE / CYBER SECURITY, OR MATHEMATICS WITH A MINIMUM OF 6 CREDIT HOURS OF STRUCTURED PROGRAMMING.
>
> **(4)** IT IS PREFERRED THAT OFFICERS HAVE DOCUMENTED EXPERIENCE IN THE CYBER MISSION FORCE (CyMF). THE VTIP PACKET MFR MEMORANDUM FOR RECORD (5.D) SHOULD INCLUDE A DESCRIPTION OF CyMF EXPERIENCE, CYBER MISSION FORCE WORK ROLE TRAINING, AND CERTIFICATION RECORDS. (DA, 2014c)

While the identification of these qualifications for eligibility does not specify any MOSs or preferred population sets, it definitely narrowed down the scope. Prior to the publication of this MILPER message, as observed in both the Cyber Career Field Update and the CF17 SME Panel, the Army knew approximately whom specifically they wanted to target for recruitment and where they wanted to recruit them from, see the highlighted portion of Figure 9:



AMERICA'S ARMY:
THE STRENGTH OF THE NATION

O-Grade (BR:94/FA:130/89)

CONCURRENT WITH MOS SME PANEL

- ➢ Create Position Code
  - Add 17A (aligned to 25A in CyMF) and 17B (35D/G) as new AOC
  - Add 17C (24A & 53A) and 17D (29A) as new FA

❑ DP: Do we merge into one AOC and/or one FA?

- ➢ Requirements Documents Review

❑ DP: What other documents besides 780/CPB we recode?

  - Recode positions on TDA change proposal to 17A/B/C/D

- ➢ Personnel Reclassifications
  - Working with ARCYBER/HRC, grant credit and reclassify officers to 17-Series

- ➢ Create 17-Series O-grade Training Course (see training way ahead)

6

UNCLASSIFIED

Figure 9. Target Population as Defined by CF17 SME Pane.
Source: CCoE (2014a).

The target population for the recruitment of future CF17 Cyber Operations Officers was defined as: 25As (Signal Officers), 35D/Gs (Military Intelligence Officers), 24As (Telecommunications Systems Engineers), 53As (Information Systems Managers), and 29As (Electronic Warfare Officers) from their respective Army Branches (CCoE, 2014a). Additionally, CMF work roles were established/described and the MOSs that could perform these duties, pre-17A, were identified as most likely candidates.

b. Target Attributes

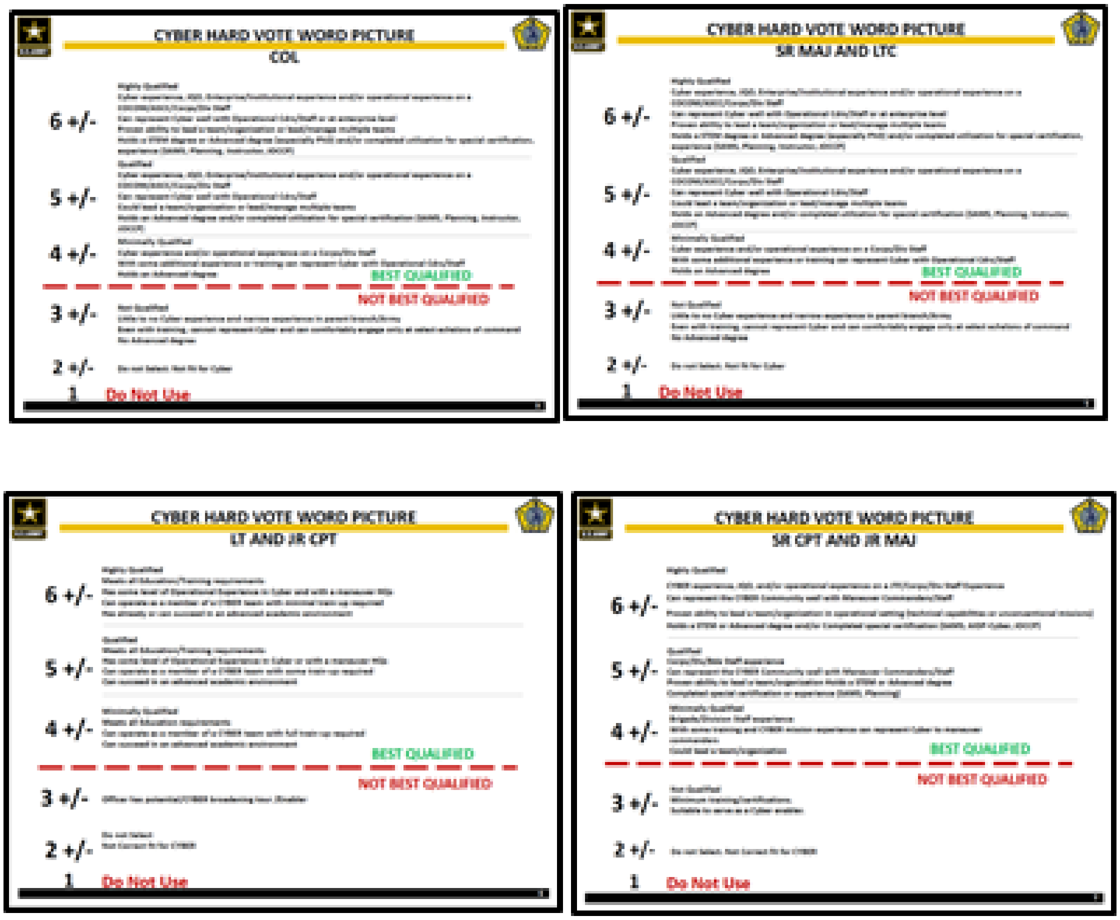
In addition to the attributes identified in the CF17 SME Panel, attributes were identified in the DA PAM 600–3, the Officer VTIP Analysis and the VTIP Scoring Criteria. The DA PAM 600–3 outlined what they call "unique attributes for Cyber Officers" as:

> (1) **Terrain sense.** Terrain sense is the ability to visualize, both physically and virtually, the battlefield and understand how to optimize cyberspace and EW weapon systems and the application of fires in the cyberspace domain. **This includes understanding the nuances of the three cyberspace layers (physical, logical, and cyber-persona) and all warfighting domains and their impacts on conducting effective cyberspace and EW operations.**

> (2) **Attention to detail.** Cyber officers must possess and demonstrate a high degree of attention to detail to ensure timely and effective delivery of cyberspace and EW operations capabilities, especially since they control capabilities that have the potential to affect systems beyond designated targets.
>
> (3) **Joint and expeditionary mindsets.** All Cyber leaders must be ready to provide cyberspace and EW operations capabilities anywhere in the world, in either long or short duration and in a flexible and adaptive manner. The application of cyberspace and EW operations includes JIIM assets that must be synchronized and synergized in support of ULO. Cyber officers must gain in-depth knowledge in the disciplines of cyberspace and EW operations, as well as, learning the nuances of JIIM planning, CEMA elements, and support to DODIN operations. This life-long learning effort starts prior to commissioning and continues throughout the officer's career. The study of foreign cultures, language skills, and formal schooling (both military and civilian) are just a few of the opportunities that will assist a Cyber officer in developing Joint and expeditionary mindsets. (DA, 2014a)

While these attributes are more heuristic than quantitatively measurable, they provide some context for the justification and identification of the attributes. For example, terrain sense can infer attributes for experience in the cyber career field. Attention to detail, while vague, justifies characteristics of individuals who have educational backgrounds in STEM. Lastly, joint and expeditionary mindsets can infer a preference for operational experience and leadership skills.

In the initial Cyber VTIP scoring criteria, Figure 10 shows the attributes that were outlined for panel members to select best qualified officers by rank:



CYBER HARD VOTE WORD PICTURE
COL

6 +/- Highly Qualified [illegible]

5 +/- Qualified [illegible]

4 +/- Minimally Qualified [illegible]

BEST QUALIFIED

NOT BEST QUALIFIED

3 +/- Not Qualified [illegible]

2 +/- [illegible]

1 Do Not Use

CYBER HARD VOTE WORD PICTURE
SR MAJ AND LTC

6 +/- Highly Qualified [illegible]

5 +/- Qualified [illegible]

4 +/- Minimally Qualified [illegible]

BEST QUALIFIED

NOT BEST QUALIFIED

3 +/- Not Qualified [illegible]

2 +/- [illegible]

1 Do Not Use

CYBER HARD VOTE WORD PICTURE
LT AND JR CPT

6 +/- Highly Qualified [illegible]

5 +/- Qualified [illegible]

4 +/- Minimally Qualified [illegible]

BEST QUALIFIED

NOT BEST QUALIFIED

3 +/- [illegible]

2 +/- [illegible]

1 Do Not Use

CYBER HARD VOTE WORD PICTURE
SR CPT AND JR MAJ

6 +/- Highly Qualified [illegible]

5 +/- Qualified [illegible]

4 +/- Minimally Qualified [illegible]

BEST QUALIFIED

NOT BEST QUALIFIED

3 +/- Not Qualified [illegible]

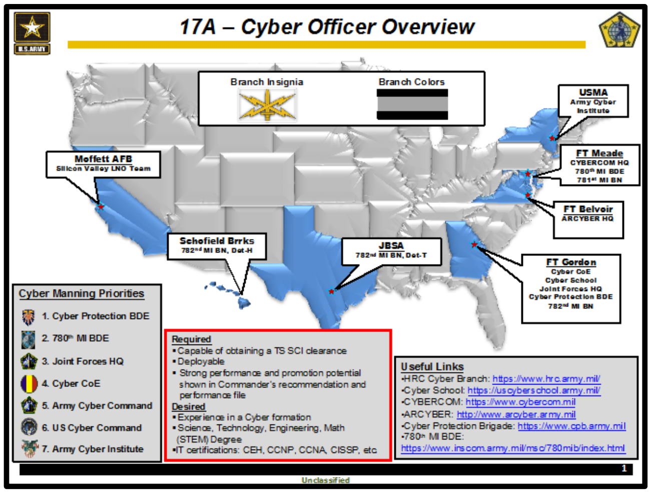
2 +/- [illegible]

1 Do Not Use

Figure 10. VTIP Scoring Criteria by Rank.
Source: Human Resources Command–Cyber [HRC–Cyber] (2015).

Again, as with attributes identified by the DA-PAM, some of these are heuristic, however these criteria do identify measurable attributes as well. These include: Cyber experience, STEM degree, institutional experience, operational experience, leadership experience.

Lastly, in the Cyber Road Show slide, provided by the HRC–Cyber, they specifically identify attributes as "required" and "desired," highlighted in Figure 11 in the box outlined in red.



17A – Cyber Officer Overview

Cyber Manning Priorities

1. Cyber Protection BDE
2. 780th MI BDE
3. Joint Forces HQ
4. Cyber CoE
5. Army Cyber Command
6. US Cyber Command
7. Army Cyber Institute

Required
- Capable of obtaining a TS SCI clearance
- Deployable
- Strong performance and promotion potential shown in Commander's recommendation and performance file

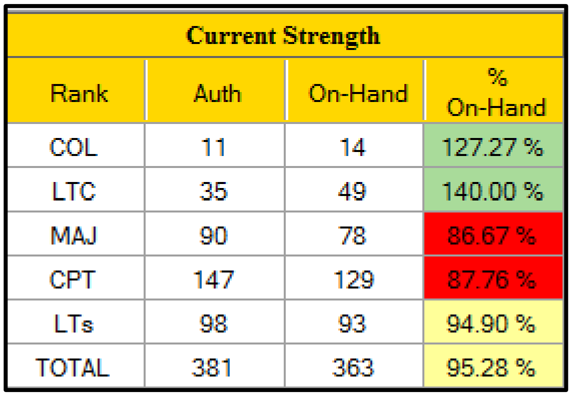
Desired
- Experience in a Cyber formation
- Science, Technology, Engineering, Math (STEM) Degree
- IT certifications: CEH, CCNP, CCNA, CISSP, etc

Useful Links
- HRC Cyber Branch: https://www.hrc.army.mil/
- Cyber School: https://uscyberschool.army.mil/
- CYBERCOM: https://www.cybercom.mil
- ARCYBER: http://www.arcyber.army.mil
- Cyber Protection Brigade: https://www.cpb.army.mil
- 780th MI BDE: https://www.inscom.army.mil/msc/780mib/index.html

Figure 11. Cyber Road Show Required and Desired Attributes.
Source: HRC–Cyber (n.d.)

c. Target Manning

The target manning for the recruitment of Cyber Operations Officers was introduced in the CF17 SME Panel, and laid out in the initial 17A Dashboard provided by HRC–Cyber as of May 4, 2016, the dashboard is shown in Figure 12:



Current Strength			
Rank	Auth	On-Hand	% On-Hand
COL	11	14	127.27 %
LTC	35	49	140.00 %
MAJ	90	78	86.67 %
CPT	147	129	87.76 %
LTs	98	93	94.90 %
TOTAL	381	363	95.28 %

Figure 12. 17A Authorization/Target Manning Dashboard.
Source: HRC–Cyber (2016).

These numbers were updated during the conduct of our research. However, we will use this dashboard in order to maintain consistency with our baseline and the actual 17A cohort whom our research focuses on. Additionally, our research will base “should hit” data for manning on the percentage of total authorized population by rank, calculated by dividing "Rank Auth" by "Total Auth," not by percentage on-hand. In this case, according to this HRC–Cyber dashboard the manning percentages of 17A total population are: COL ~ 3%, LTC ~ 9%, MAJ ~ 24%, CPT ~ 38%, and LTs ~ 26%. These are the percentages we use for "should hit" data for manning.

(2) The Selection Process

Our research covers the first two VTIPs conducted by the U.S. Army to select the first cohort of Cyber Operations Officers. The first two rounds of VTIP occurred in the first and third quarters of fiscal year 2015 and a total of 1,230 individuals applied, with 327 being selected. Also of note, 172 officers not selected during the first VTIP reapplied in the second and 54 of them were selected in the second VTIP (CCoE, n.d.). Three primary reasons for non-selection were identified by CCoE: 1) previous performance, 2) lack of desired technical skills/experience and 3) year group eligibility cut lines. We were not able to access any previous performance information on selected officers or year group eligibility cut lines for them, so our focus was on the reason number two: lack of desired skills/experience. For our research, the desired skills/experience identified in the Cyber VTIP scoring criteria and the Cyber Road show, equal target attributes. Additionally, the selection process only involved a review of the applicants file which included: Officer Evaluation Reports (OER) for performance review, Officer Record Briefs (ORB) for experience review, and VTIP application for a limited review of skill. The VTIP application process did not include an aptitude assessment test, skill validation or interview.

(3) U.S. Army Cyber Work Roles (17A Duties and Responsibilities)

The duties and responsibilities of the Cyber Operations Officer were published in the DA PAM 600–3 by the CCoE. Additionally, these roles were identified and described in detail by a working group for defining cyber work roles. In this working group, they came up with eight cyber work roles for the 17A: Cyber Network Defense (CND) Manager, Sub-element Lead, Operations Officer, Remote Operator, Cyber Operations Planner, Cyber Capability Developer, Cyber Defense Analyst and Team Lead

(ARCYBER, n.d.(b)) This working group also detailed the duty descriptions for each of these work roles, along with work role requirements, recommended certifications and recommended civilian education.

5. Measures of Effectiveness

a. Factor Analysis

Based on information discovered in our literature review and our combined operational experiences we developed what we felt were suitable MOEs for evaluating the effects of the Army's recruitment of the Cyber Operations Officer. Our first MOE, job satisfaction was introduced by Rashmi (2010) as a metric that could be used to measure the success of the recruitment process, he specifically explains that this metric can be collected from a candidate survey and used as a data point to demonstrate the actual value of the whole recruitment process. For our second MOE, the assessment of the recruitment process, we looked at Guest's HRM model where he specifically discussed the role "public image" plays in the recruitment process, highlighting that an organization with a reputation for distinctively treating their employees well during the recruitment process, maximizes the quality of work dimension of that organization (Guest, 1987). Lastly, our third MOE, motivation, was developed by our combined 32 years of military experience teaching us the value of having motivated officers as part of our formations. Therefore, we believe that knowing the motivations of the members of your organization is a great way to measure the effects of a recruitment strategy.

We developed sections of our survey questionnaire to address these MOEs and attempt to measure the effects of the Army's recruitment of Cyber Operations Officers based on these measures. For context, we provide an explanation of each:

a) MOE 1—Job satisfaction: this MOE addresses how respondents felt about how expectations developed during the recruitment process compared to the reality of the job, confidence levels in their technical abilities to perform their assigned duties and their perception of opportunities for advancement.

b) MOE 2—The assessment of the recruitment process: this MOE addresses how respondents felt about the actual recruitment process. It inquires specifically about their impressions of the application packet, the support of their chain of command during the process and communication with HRC–Cyber during the process.

c) MOE 3—Motivation: this MOE addresses respondent's motive for becoming a 17A, specifically inquiring about their passion, technical experience, future career goals, satisfaction with their previous MOS (if applicable) and opportunities for advancement.

We developed multiple questions to measure each of these MOEs: MOEs 1 and 2 contain three questions each, and MOE 3 contains five. The questions associated with these MOEs are represented by the number of survey prompts associated with them. Question numbers, 21a–21c in Table 3, address MOE 1, the respondent's job satisfaction; 20a–20c address MOE 2, the respondent's assessment of the recruitment process; and 36a–36e address MOE 3, the respondent's motivation. Responses to all survey prompts regarding these MOEs were on the Likert scale with possible responses of agree (A), strongly agree (SA), neutral (N), disagree (DA), strongly disagree (SDA) or N/A.

In order to verify the suitability of our proposed MOEs, in coordination with TRAC–Monterey, we conducted exploratory factor analysis (EFA) to determine the impact of our MOEs on the variance of our survey data. We use this analysis of our proxy MOEs to evaluate the effects of the Army's recruitment strategy in the Cyber Branch.

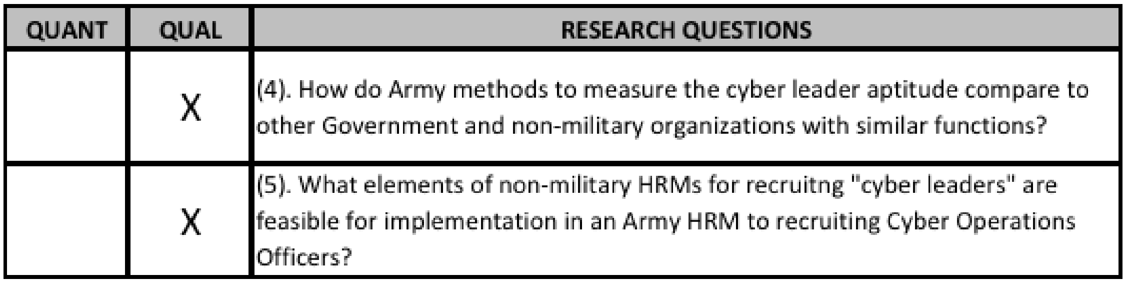
b. Sentiment/Text Analysis

On the qualitative side of the 17A survey there were three open-ended questions, item numbers 38, 39 and 40 in Table 3. These questions asked respondents to provide feedback on the difficulties of the recruitment process, recommendations for improvement and recommendations for additional topics to address outside of those covered in the survey. In partnership with TRAC–Monterey we conducted basic sentiment and text analysis of these responses to provide some additional context for our MOEs and the evaluation of the recruitment process. According to Luo et al., sentiment analysis refers to "the application of natural language processing, computational linguistics, and text analytics to identify and classify subjective opinions in source materials" (Lou et al., 2013, p. 53). Based on response rates to these questions we decided to only use question numbers 38 and 39 for the analysis, question number 40 did not have a sufficient response rate to conduct reliable sentiment analysis. A manual text analysis was conducted of all open-ended responses and placed in one of three categories: recruitment related (responses related to the creation of a pool of potential candidates), selection related (responses related to how individuals were chosen from the pool of potential candidates), and none (for individuals that said they had no issues or difficulties with either part of the process). Question numbers 38 and 39 were analyzed separately and together to gain insight into the respondents' opinions, attitudes and disposition regarding the recruitment and/or selection processes. In addition, we include some direct quotes from the survey to capture common sentiments shared among respondents that shed light on the effects of the Army's recruitment strategy in the Cyber Branch.

6. Data Collected from Other Government and Non-government Organizations

Other Government agencies and private companies require personnel with the same set of skills and education as Cyber Operations Officers. Data collected from these organizations allows the researchers to compare recruitment models and targeted personnel attributes. Recall that offensive cyber activities are considered illegal when conducted by private companies and some Federal Government agencies. The comparative analysis is restricted to cyber activities conducted by the Federal Government, U.S. Army, and private companies. Data collected from the Department of Homeland Security (DHS) and Facebook assisted with answering the research questions in Table 7.

Table 7. Research Questions Addressed by Other Government and Non-government Organizations



QUANT	QUAL	RESEARCH QUESTIONS
	X	(4). How do Army methods to measure the cyber leader aptitude compare to other Government and non-military organizations with similar functions?
	X	(5). What elements of non-military HRMs for recruitng "cyber leaders" are feasible for implementation in an Army HRM to recruiting Cyber Operations Officers?

These data are used to identify the selection criteria, application, and candidate evaluation process utilized by non-military and non-government organizations. Most importantly, this data illustrates the metrics used by these organizations. This allows the authors to evaluate the methods for use within the military HRM.

C. COMPARATIVE ANALYSIS

The purpose of the comparative analysis portion is to compare the aspects of the Army Cyber Operations Officer recruitment process to those of selected companies. The intent is to compare and contrast relevant components where possible and highlight the most impactful differences due to the capacity or environments in which the entities operate. To achieve this, a baseline is established for the HRMs used, targeted attributes, and recruitment processes utilized by the Army, governmental, and non-governmental organizations. The HRMs will be categorized and evaluated based on the constructs and models outlined in Chapter II. This sets the stage for an evaluation of the constructs and models utilized by the Army, DHS, and Facebook to meet their respective Cyber workforce needs.

Next, an analysis of how the aforementioned organizations develop their respective recruiting pools is conducted. A baseline for targeted attributes is established with discussion on, and caveats, for legal authorities. An analysis of how targeted attributes impact and are impacted by the HRM in which the attributes exist is also included in this portion of the comparative analysis. For example, a discussion of available mechanisms and tools, such as aptitude or physical testing, to make the recruitment pool manageable and eliminate undesirable candidates is a subset of this portion of the comparative analysis.

Finally, an analysis of the recruitment and selection process utilized by the Army, DHS, and Facebook is conducted. The Army VTIP is compared with the practices of governmental, non-governmental, and agreed upon best business practices of the cybersecurity industry. Based on the recruiting pool developed by the respective organizations and under the confines of the utilized HRMs, the selection processes are compared side by side to. The goal is to highlight differences and similarities due to HRM operating environments and legal considerations.

The goal of the comparative analysis is to identify and understand the factors that affect how organizations recruit and select personnel to provide the requisite cybersecurity capabilities. An analysis of established industry practices and developed recruitment mechanisms lays the foundation for the incorporation of different HRMs, attributes, and/or selection processes to improve Army Cyber Operations Officer recruitment efficiency and efficacy.

D. SUMMARY

To answer our research questions, we approached from both quantitative and qualitative perspectives. The quantitative data consisted of survey responses from the 17A population and population demongrahics reported by the Army in PDE. MOEs were introduced with the intent to validate through factor analysis and evaluate the effectiveness of the Cyber Operations recruitment process quantitatively. Additionally, this chapter provided an explanation of our use of case studies for non-military and civilian organizations that require similar skills to understand how the recruiting environment affects cybsecurity recruiting processes. We also compared Cyber Operations Officer recruitment with other Army specialty recruiting, non-military, and civilian organizations to understand the linkages between function and HRM model. The data is analyzed in this manner to evaluate the effectiveness of the Army's recruitment processes for 17As and compare those processes with best business practices.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. QUANTITATIVE RESEARCH FINDINGS

This chapter includes results from our quantitative research methods. The quantitative findings will address how well the Army is recruiting 17As, which our research refers to as MOPs. The MOP analysis is an evaluation of the Army strategy's effectiveness as it pertains to achieving its recruitment goals, and addresses the question "Are they accomplishing tasks to standard?." Additionally, we will detail our quantitative findings regarding the effects of the Army achieving their recruitment goals on the cyber branch to date, as it pertains to the current 17A population, which our research refers to as MOEs. The MOE analysis is an evaluation of the Army recruitment strategy's effect on the cyber branch, and addresses the question, "Are they creating the effect(s) or conditions in the OE that they desire?" We also analyze the PDE data to both validate demographic data for the 17A survey and conduct descriptive statistical analysis to identify current population of 17As as they compare to the larger Army demographic.

A. "SHOULD HIT" DATA—ARMY INSTITUTIONS

The information provided from Army cyber related institutions gave us our "should hit" data. This analysis allows us to establish the critical benchmarks for which we base our evaluation of the Army's recruitment of Cyber Operations Officers, specifically, how effective have they been in achieving their recruitment goals. We grouped our findings for these recruitment goals into three categories which are identified as follows:

1. **Target population—**The Army wanted to create the 17 series position code by aligning it with 25As (Signal Officers), 35D/Gs (Military Intelligence Officers), 24As (Telecommunications Systems Engineers), 53As (Information Systems Managers), and 29As (Electronic Warfare Officers) from their respective Army Branches. This was the target population of their recruitment strategy.
2. **Target attributes—**The target attributes for recruitment of 17As, in order of their outlined priorities are: cyber experience, operational/ leadership

experience, STEM degrees and IT Certifications.

3. **Target manning—**For our research we identify the target manning as a percentage of total population by rank. The Army's target manning for their recruitment strategy was: COL ~ 3% , LTC ~ 9%, MAJ ~ 24%, CPT ~ 38%, and LTs ~ 26%.

Additionally, from our analysis we were able to determine how these overarching recruitment goals were prioritized as well as some of the priorities within the recruitment goals.

B. "DID HIT" DATA—17A SURVEY RESULTS

The 17A web-based survey was our primary data collection tool, and supports both quantitative and qualitative analysis. Data collected from this survey was used to analyze:

- How well the Army is performing its 17A recruitment (MOPs)
- How effective has the Army's recruitment of 17As been to date. (MOEs)
    a. Factor analysis and regression tree
    b. Sentiment analysis

1. Measures of Performance

Our analysis for the evaluation of the Army's Strategy for recruiting Cyber Operations Officers begins with the MOP assessment of "should hit" and "did hit" data. For this assessment we used the findings from our analysis of data from Army institutions on their goals for recruiting Cyber Operations Officers and identified what percentage of the current 17A population represent that goal. The target goals we specifically observed in this survey were:

a. Population: previous MOS

b. Attributes: Cyber experience, operational/leadership experience, STEM degrees and IT certifications

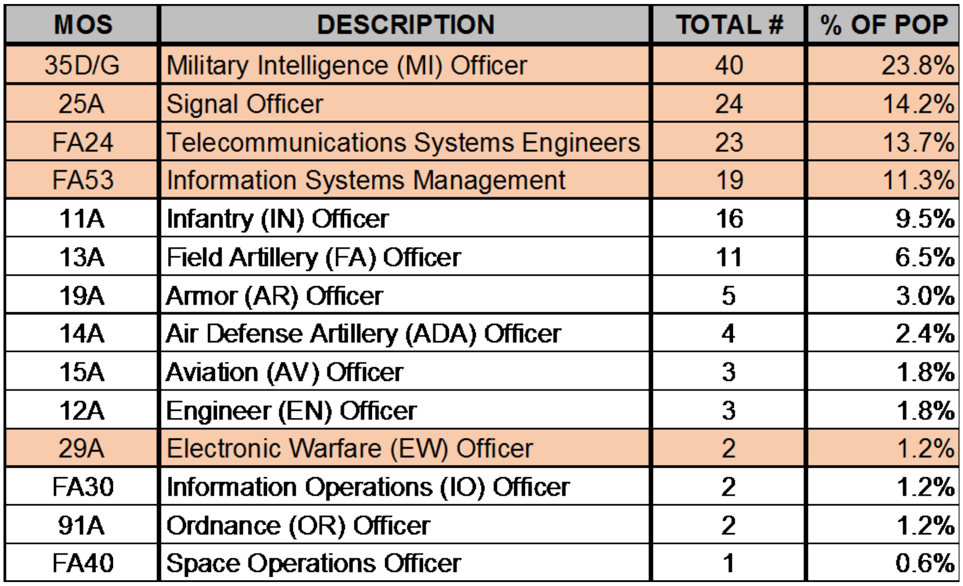
c. Manning: rank (percentage of population).

Additionally, we analyzed if the priorities outlined by the Army's strategy for the recruitment of Cyber Operations officers align with the results of the survey based on the survey results. No defined threshold for recruitment success was identified by any Army institutions in the data that we were able to collect. As a result, we developed this threshold using both the Joint Staff's (2011b) *Commander's Handbook for Assessment Planning and Execution* and the Office of Personnel Management's (n.d.) Performance Management Cycle. From these two sources we were able to identify steps to develop threshold criteria and specify and apply measures to elements which we were evaluating. For our analysis, we define the threshold for a target goal being SUCCESSFUL as achieving 85% or higher of the targeted goal, an achievement rate below 85% will be considered UNSUCCESSFUL. The survey prioritization of target goals will be determined by achieved percentage of goals, the higher the percentage, the higher the priority, i.e., if Goal A has a 92% achieved rate and Goal B has a 97% achieved rate, Goal B would be considered a higher priority than Goal A.

a. Target Population

For target population, the Army identified that they planned to align CF17 with 25As, 35D/Gs, 24As, 53As and 29As. Question 16 asks "What was your previous MOS, if applicable?" and the question was applicable to 87% of the respondents and Table 5 shows the breakdown of this population.

Table 8. Survey Results, Previous MOS



MOS	DESCRIPTION	TOTAL #	% OF POP
35D/G	Military Intelligence (MI) Officer	40	23.8%
25A	Signal Officer	24	14.2%
FA24	Telecommunications Systems Engineers	23	13.7%
FA53	Information Systems Management	19	11.3%
11A	Infantry (IN) Officer	16	9.5%
13A	Field Artillery (FA) Officer	11	6.5%
19A	Armor (AR) Officer	5	3.0%
14A	Air Defense Artillery (ADA) Officer	4	2.4%
15A	Aviation (AV) Officer	3	1.8%
12A	Engineer (EN) Officer	3	1.8%
29A	Electronic Warfare (EW) Officer	2	1.2%
FA30	Information Operations (IO) Officer	2	1.2%
91A	Ordnance (OR) Officer	2	1.2%
FA40	Space Operations Officer	1	0.6%

Table 8 shows that 64% of the 17As that had previous MOSs were from the target population identified by the Army's recruitment strategy. This makes this target goal UNSUCCESSFUL. Based on our analysis the cause for this deficiency can be attributed to a change of course with regard to the original implementation plan for the CF17 alignment (see Figure 8). At some point the plan to target five specific MOSs and/or functional area officers based on presumed skill sets was adjusted to include additional MOSs and functional areas, reflected in Table 7. While our research did not obtain data on specific adjustments to this alignment, the current state of the branch as well as other MOSs and functional areas identified in Figure 8 would suggest that the plan was modified or unable to be met.

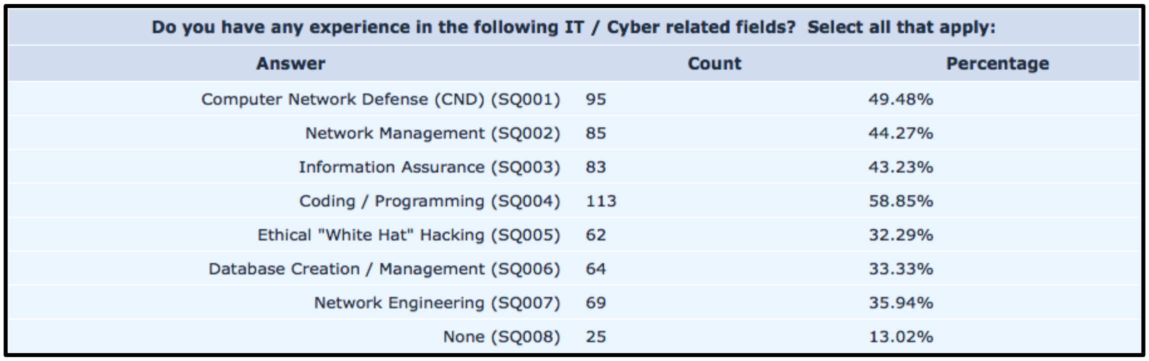
b. Target Attributes

For target attributes, the Army's strategy outlined the desired attributes, in order of priority as: Cyber experience, operational/leadership experience, STEM degree, IT Certifications. Ten survey questions address the attributes of the respondents; we will begin with cyber experience.

(1) Cyber Experience

For the purpose of our research, we equate “cyber experience” to “experience in IT/Cyber related fields” and Question 17 (Table 3) asks, “Do you have any experience in the following IT/Cyber related fields?” Table 9 shows the breakout of the responses.

Table 9. Survey Results, Cyber Experience



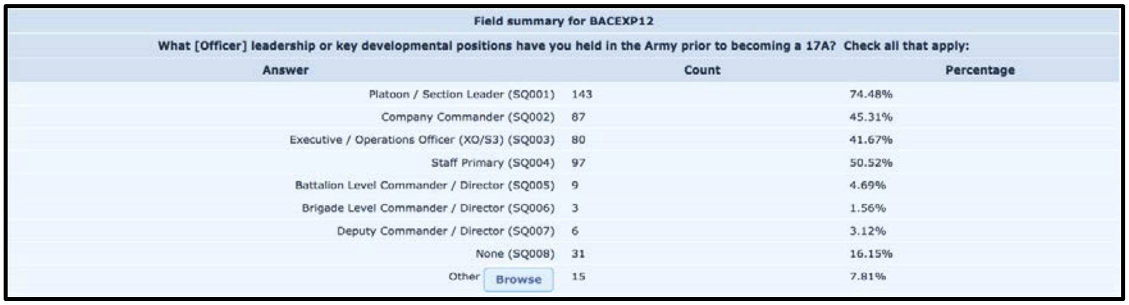
Do you have any experience in the following IT / Cyber related fields? Select all that apply:		
Answer	**Count**	**Percentage**
Computer Network Defense (CND) (SQ001)	95	49.48%
Network Management (SQ002)	85	44.27%
Information Assurance (SQ003)	83	43.23%
Coding / Programming (SQ004)	113	58.85%
Ethical "White Hat" Hacking (SQ005)	62	32.29%
Database Creation / Management (SQ006)	64	33.33%
Network Engineering (SQ007)	69	35.94%
None (SQ008)	25	13.02%

According to Table 8, 87% of respondents had some experience in IT/Cyber related fields, with almost 60% having experience with coding/programming. This would make the Army’s target goal of recruiting personnel with cyber experience SUCCESSFUL. Our analysis shows that cyber experience was a high value attribute, consistently identified as a requirement for potential 17As. Our survey results confirm the emphasis placed on this attribute by the Cyber branch. Additionally, of the 13% of survey respondents without cyber experience, field grade officers (MAJ, LTC and COL) accounted for 56% while company grade officers (2LT, 1LT and CPT) accounted for 44%. This suggests, that while there is not a significant discrepancy between rank and this specific attribute, field grade officers exceed their proportional representation in lacking cyber experience.

(2) Operational/Leadership Experience

Operational/leadership experience was identified as the next desired attribute, question 18 (Table 3) asks, “What [Officer] leadership or key developmental positions have you held in the Army prior to becoming a 17A?” Table 10 details the responses to this question.

Table 10. Survey Results, Operational/Leadership Experience



Field summary for BACEXP12

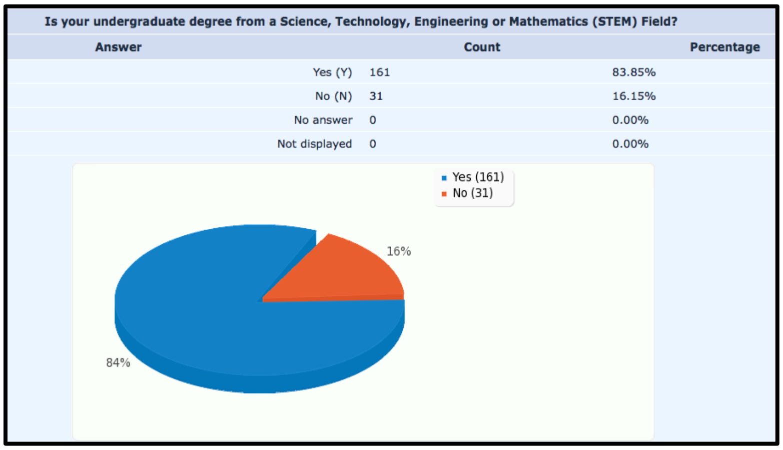
What [Officer] leadership or key developmental positions have you held in the Army prior to becoming a 17A? Check all that apply:

Answer	Count	Percentage
Platoon / Section Leader (SQ001)	143	74.48%
Company Commander (SQ002)	87	45.31%
Executive / Operations Officer (XO/S3) (SQ003)	80	41.67%
Staff Primary (SQ004)	97	50.52%
Battalion Level Commander / Director (SQ005)	9	4.69%
Brigade Level Commander / Director (SQ006)	3	1.56%
Deputy Commander / Director (SQ007)	6	3.12%
None (SQ008)	31	16.15%
Other Browse	15	7.81%

Table 10 shows that 84% of respondents have some operational/leadership experience, with over 45% with at least company command. This attribute just misses the threshold requirement for success and is therefore UNSUCCESSFUL. Our analysis shows that the cause for this deficiency can mostly be attributed to the proportion of company grade officers without operational/leadership experience. Company grade officers, as expected, account for 100% of the survey respondents without operational/leadership experience.

(3) STEM Degrees

Although STEM degrees were noted as "preferred" not required in most documentation provided by the Army institutions we collected data from, it was a consistently identified attribute, which is why we identified it as a target goal. There are six survey questions that address STEM degrees, either at the undergraduate or graduate levels Figure 13 details the responses for individuals with STEM undergraduate degrees.



Is your undergraduate degree from a Science, Technology, Engineering or Mathematics (STEM) Field?

Answer	Count	Percentage
Yes (Y)	161	83.85%
No (N)	31	16.15%
No answer	0	0.00%
Not displayed	0	0.00%

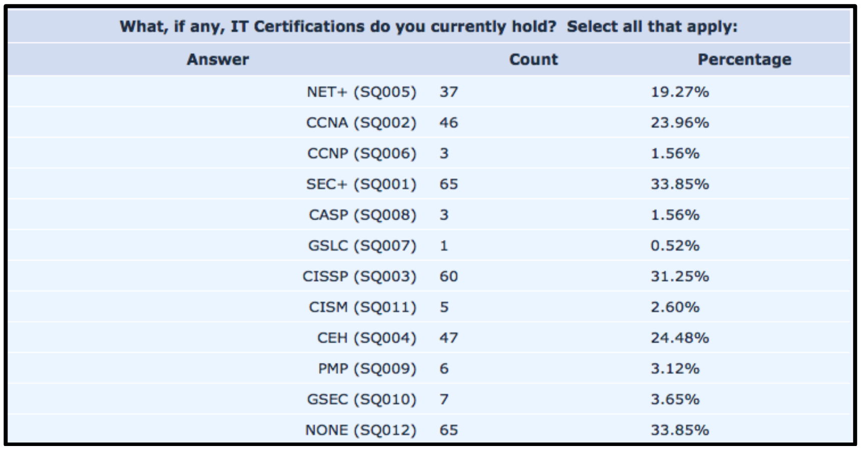
Figure 13. Survey Results, STEM Degrees

Navigating through the data provided by this survey we were able to determine that 11 of the 31 respondents without undergraduate STEM degrees, had graduate STEM degrees. Bringing the total to 172, or 90% of respondents had either an undergraduate or graduate STEM degree. Therefore, the Army was SUCCESSFUL at achieving their target goal of recruiting personnel with STEM degrees. Of the remaining 10% of respondents with neither an undergraduate or graduate STEM degree, 80% were field grade officers, with the remaining 20% being company grade officers. The STEM degree attribute is the second attribute that field grade officers exceed their proportional representations in lacking a desired attribute.

(4) IT Certifications

Holding an IT certification is not an attribute explicitly required by any data collected from Army institutions for this research. However, both the Cyber Work Role working group and the Cyber Road Show presentations identify IT certifications as a desired attribute for Cyber Operations Officers. As a result, our research makes IT certifications the lowest priority for the Army’s target attributes. To obtain this information Question 15 (Table 3) asks, “What, if any, IT Certifications do you currently hold?” Table 11 details the responses to this question.

Table 11. Survey Results, IT Certifications



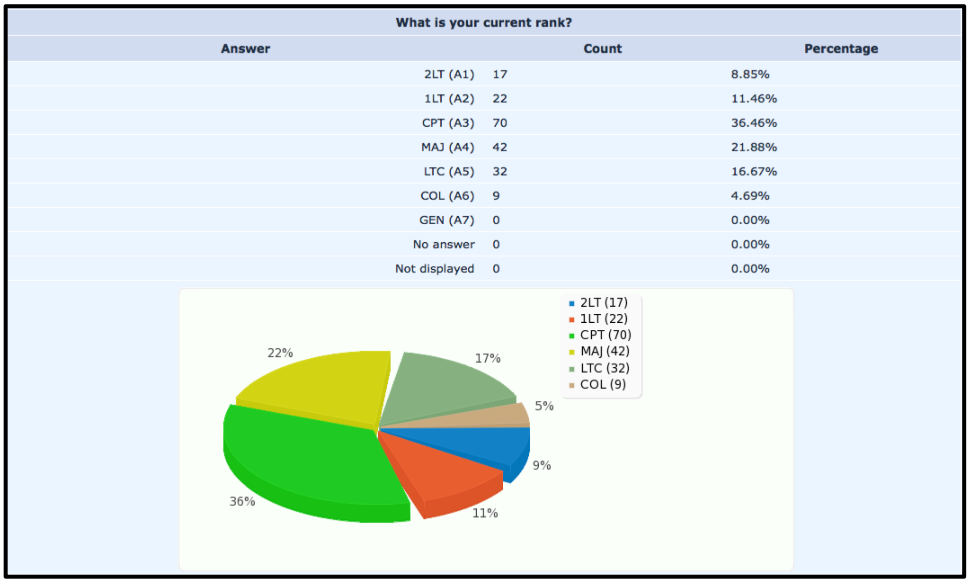
What, if any, IT Certifications do you currently hold? Select all that apply:

Answer	Count	Percentage
NET+ (SQ005)	37	19.27%
CCNA (SQ002)	46	23.96%
CCNP (SQ006)	3	1.56%
SEC+ (SQ001)	65	33.85%
CASP (SQ008)	3	1.56%
GSLC (SQ007)	1	0.52%
CISSP (SQ003)	60	31.25%
CISM (SQ011)	5	2.60%
CEH (SQ004)	47	24.48%
PMP (SQ009)	6	3.12%
GSEC (SQ010)	7	3.65%
NONE (SQ012)	65	33.85%

Table 11 shows that 67% of respondents hold at least one IT certification. Additional analysis of this data shows that the average number of certifications held by respondents with at least one certification is three. The top three certifications were SEC+, CISSP and CEH, and 33% of respondents had no certifications at all. The Army did not reach the 85% threshold for achieved rate and therefore was UNSUCCESSFUL in achieving recruitment goals for individuals with IT certifications. This can primarily be attributed to the lack of explicitly defining this attribute as required. Additionally, based on our research, IT certifications are generally considered an "acquired skill," which according to Moustroufas et al. (2015), specify actual or obtained competencies of the employee not a potential candidate. Our analysis also shows that of the ~34% of respondents without IT certifications, it was essentially a 50/50 split between field grade and company grade officers, suggesting that the Army treated this target attribute equally between all ranks.

c. Target Manning

For our research, the authoritative data source analyzed for "did hit" data for target manning is the PDE database, which will be addressed later in this chapter. However, the data collected from the PDE database will also be used to validate the demographic breakout of our survey, which is why target manning will also be addressed in this section. The survey question used to ask respondents about rank was a basic demographic question, Question 5 (Table 3) asks, “What is your current rank?” Figure 14 details the responses to this question.



What is your current rank?

Answer	Count	Percentage
2LT (A1)	17	8.85%
1LT (A2)	22	11.46%
CPT (A3)	70	36.46%
MAJ (A4)	42	21.88%
LTC (A5)	32	16.67%
COL (A6)	9	4.69%
GEN (A7)	0	0.00%
No answer	0	0.00%
Not displayed	0	0.00%

Figure 14. Survey Results, Rank Demographic

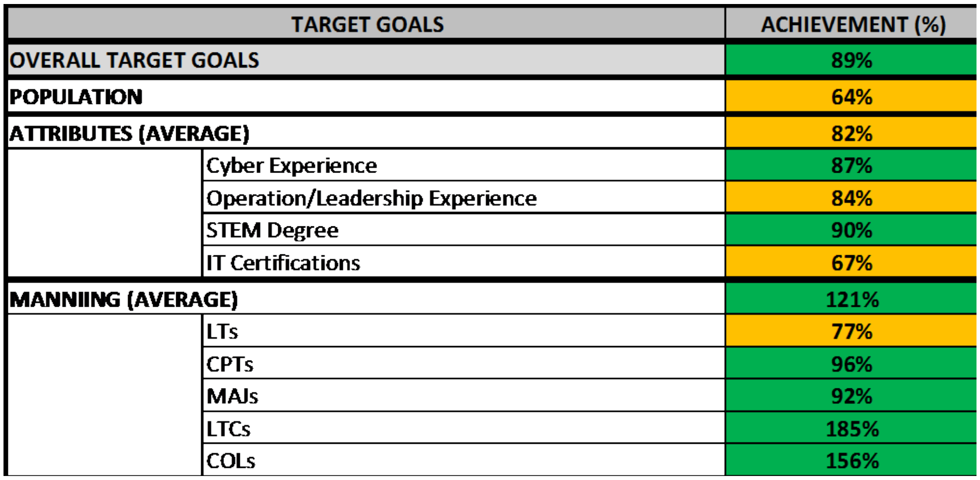
According to Figure 14 the Army was SUCCESSFUL in achieving its recruitment goals for target manning (+/- 3%) for COLs, LTCs, MAJs and CPTs. They were UNSUCCESSFUL in achieving recruitment goals for 2LTs and 1LTs, achieving 20% of the targeted 26%, which is less than the 85% achieved rate established as the threshold. Additionally, the Army over-performed on the recruitment of LTCs and COLs by almost 10% or 175% achieved rate. Through our analysis we attribute this to the fact that the Army’s initial recruitment strategy focused primarily on the traditional VTIP process allowing senior officers to become a larger part of the pool of potential candidates and increasing the chances of selection as rank increased, while providing a secondary focus on accessions into the branch**.**

d. MOP Summary

In summary, the Army reached an 89% achievement rate overall in “accomplishing tasks to standard” or achieving its targeted recruitment goals. There were only four of ten measured areas where they were UNSUCCESSFUL in reaching an 85%

achievement rate of recruitment goals: target population; target attributes for operational/leadership experience and IT certifications; and target manning for LTs. As a result, we conclude that the Army was effective in creating an applicant pool of potential candidates for selection of 17As, however, based on some of the observed discrepancies by rank, we conclude that the selection process did not effectively differentiate between applicants in order to objectively select those with greater qualifications. Table 12 provides a visual summary of these findings.

Table 12. MOP Summary



TARGET GOALS		ACHIEVEMENT (%)
OVERALL TARGET GOALS		89%
POPULATION		64%
ATTRIBUTES (AVERAGE)		82%
	Cyber Experience	87%
	Operation/Leadership Experience	84%
	STEM Degree	90%
	IT Certifications	67%
MANNIING (AVERAGE)		121%
	LTs	77%
	CPTs	96%
	MAJs	92%
	LTCs	185%
	COLs	156%

2. Measures of Effectiveness

a. Factor Analysis and Regression Tree Model

The results of our MOP analysis show our evaluation of the effectiveness of the recruitment strategy. Next we assess its effects in the Cyber Branch by looking at our proxy MOEs. As introduced in Chapter III, our proposed proxy MOEs are: MOE 1—job satisfaction; MOE 2—assessment of the recruitment process; and MOE 3—motivation. We decided to use factor analysis to validate our MOEs because it is viewed as an appropriate analytical tool for survey questionnaires. Factor analysis can treat multiple questions as separate consolidated variables that can be used to identify and measure underlying concepts, called latent variables (Hamilton, 1992). In our case, these underlying concepts or latent variables are our MOEs, which shape an idea for the value of the Cyber Operations Officer to the branch. As we discuss results of the exploratory factor analysis (EFA) for our MOEs in this section, it is important to explain the interaction between two important terms: MOEs and factors. For the purpose of simplifying the explanation of our EFA results, we will use the term "factors" to describe our MOEs, accordingly, Factor 1 is equivalent to MOE 1, Factor 2 is equivalent to MOE 2 and Factor 3 is equivalent to MOE 3. Variables are the remaining survey responses that can explain these Factors.

TRAC–Monterey assisted us with conducting our EFA using the software program "R," which is "a language and environment for statistical computing and graphics" (The R Foundation, n.d.). To validate our three factors, we conduct a scree test on all survey results which produce a line segment plot (Figure 15), called a "scree plot." Scree plots identify important factors that represent the fraction of total variance in the data (The R Foundation, 2017). This plot provides a visualization that distinguishes important factors from other factors that can be ignored. This distinction is illustrated with the flattening of the slope in the plot, sometimes referred to as the "elbow" (The R Foundation, n.d.). In our scree plot the "elbow" occurs after the third factor (labeled OC in Figure 15), which coincides with our decision to use three factors (MOEs) for analysis.

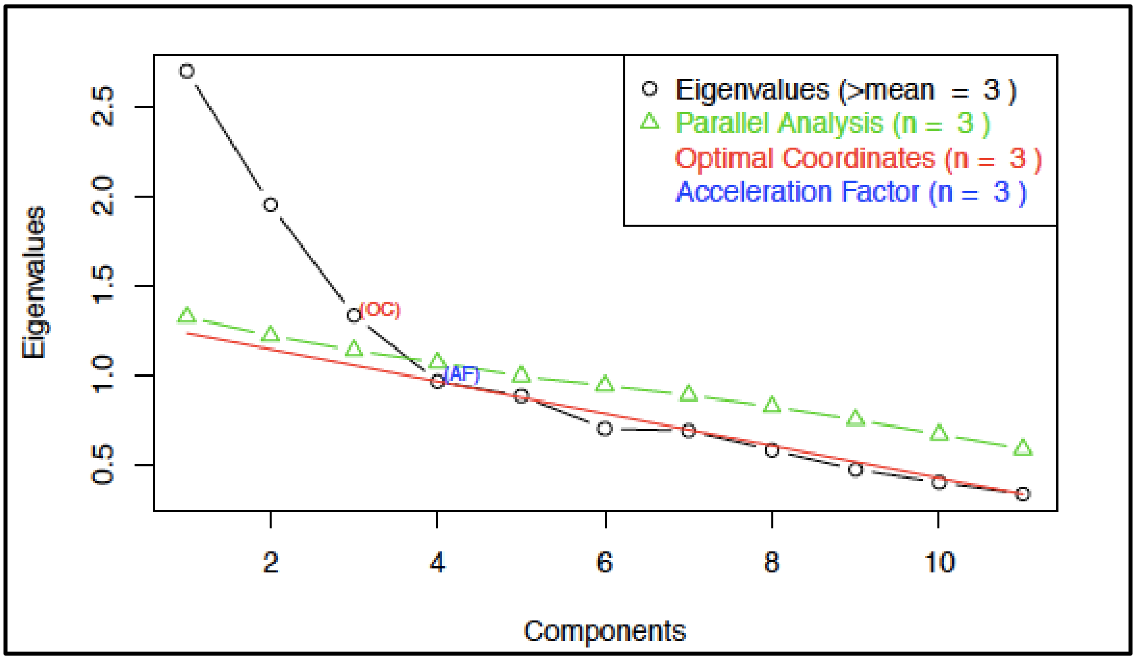


Figure 15. Scree Plot for 17A Survey Results

Next, the aggregated responses to our 17A survey were analyzed using our correlation matrix (Figure 16) and rotated using the “varimax” criterion.

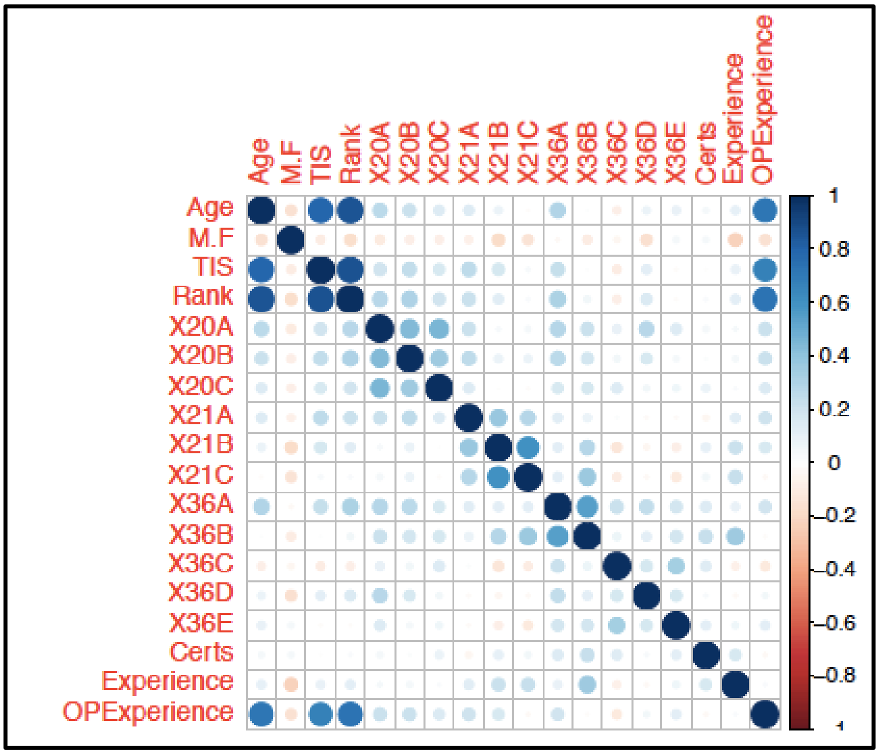
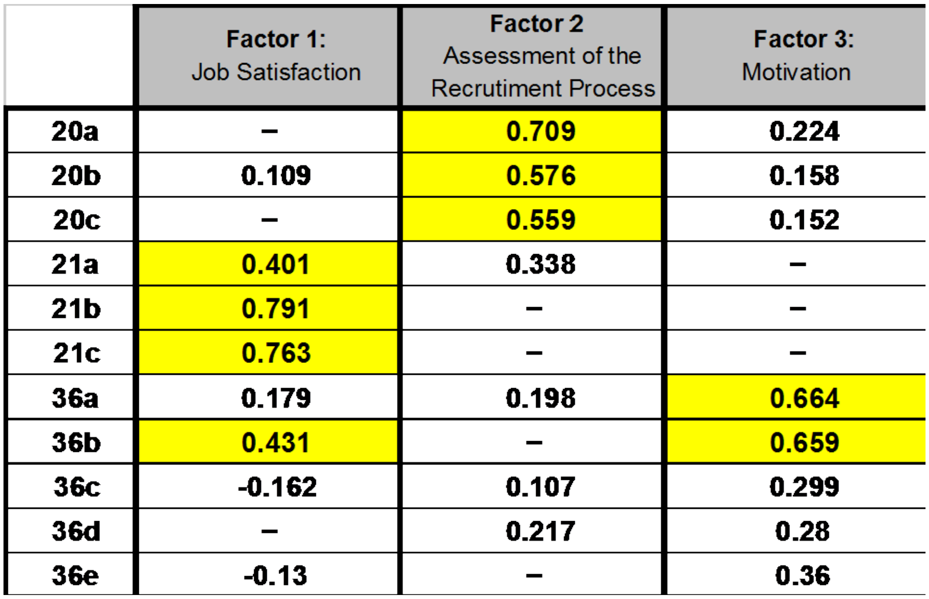


Figure 16. 17A Survey Correlation Matrix Used for EFA

For context, varimax is a technique to further simplify loading patterns that eases the interpretation of data and the relative importance of each factor (Brown, 2009). This EFA with varimax rotation resulted in the identification of 11 variables—Questions 20a, 20b, 20c, 21a, 21b, 21c, 36a, 36b, 36c, 36d, and 36e (Table 3)—that exhibited strong correlations with the three factors. The strength of the correlation between these 11 variables and the factors is expressed by what is referred to as "factor loading" (The R Foundation, n.d.). Factor loadings can be interpreted as correlation coefficients between the variables and the Factors, "they determine the strength of the relationships" (Yong & Pearce, 2013, p. 84). They range from -1 to +1, positive numbers represent positive correlation and negative numbers represent negative correlation, and the closer the number is to -1 or +1, the greater the correlation (Rummel, 1967).

From this EFA we only use variables loading .400 or higher, highlighted in the factor loading matrix (Table 13). Factor 1, job satisfaction, had four variables that loaded .400 or higher: Questions 21a, 21b, 21c and 36b (Table 3). Although Question 36b loads at 0.431 with factor 1, we decided not to include it in the group of variables because we determine that it’s too similar to variable 21b. Variable 21b addresses having the technical skills required to perform assigned duties as expected and 36b addresses having the technical experience and expertise to excel in the Cyber Branch, this similarity along with Question 36b loading much higher for Factor 3, drives our decision not to include it in factor 1. Factor 1, on its own, accounts for 15% variation in our survey data. Factor 2, assessment of the recruitment process, loaded above .400 for three variables 20a, 20b and 20c, which include all variables we group with Factor 2. Factor 2 accounts for 12.5% of the variation of the data. Factor 3, motivation, loaded above .400 for only two variables: 36a and 36b. We grouped five variables within Factor 3, however, three of the five did not load higher than .400, which does not imply lack of significance, only that these additional variables do not add additional context to the results. Factor 3 accounted for 11.7% of variation in our survey data. These three factors along with their strongly correlated variables account for 39% of the variation within our 17A survey data set. While 39% is not an overwhelming proportion, it is significant, especially considering that the data did not include performance evaluations or other objective measurements. Additionally, the fact that the number of survey respondents represents over 51% of the 17A population, this EFA validates the use of our MOEs to evaluate the effects of the Army’s recruitment of the Cyber Operations Officer.

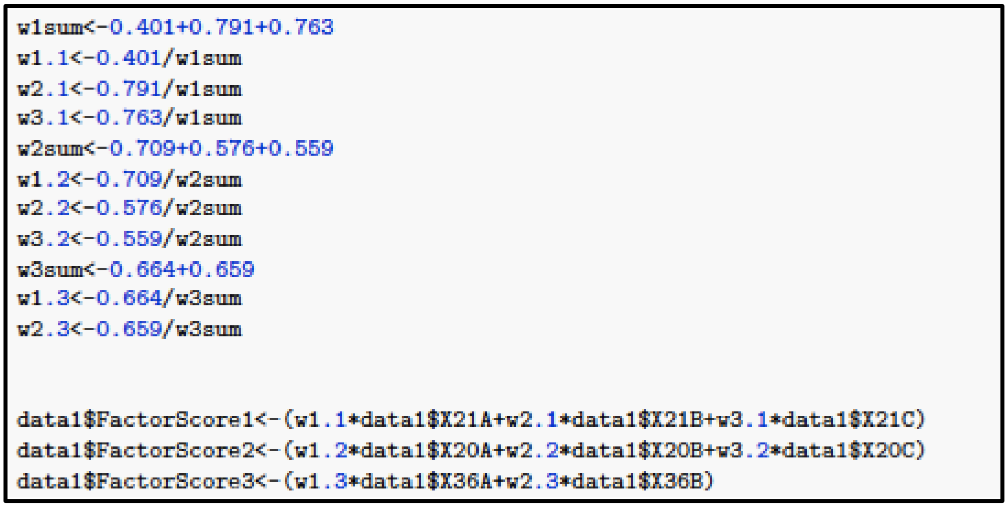
Table 13. Factor Loading Matrix for 17A Survey Factor Analysis



	Factor 1: Job Satisfaction	**Factor 2** Assessment of the Recrutiment Process	**Factor 3:** Motivation
20a	**–**	**0.709**	**0.224**
20b	**0.109**	**0.576**	**0.158**
20c	**–**	**0.559**	**0.152**
21a	**0.401**	**0.338**	**–**
21b	**0.791**	**–**	**–**
21c	**0.763**	**–**	**–**
36a	**0.179**	**0.198**	**0.664**
36b	**0.431**	**–**	**0.659**
36c	**-0.162**	**0.107**	**0.299**
36d	**–**	**0.217**	**0.28**
36e	**-0.13**	**–**	**0.36**

After validating these MOEs with EFA and correlating them with other independent variables in our data set, we worked with TRAC–Monterey to create regression tree models to predict factor responses based on the identified independent variables. Regression trees are a simplified version of linear regression which use partitioned segments of data to make quantitative predictions (Carnegie Melon University [CMU], 2006). Because of the complexity of our data and its nonlinear interactions between variables, the use of linear regression was not practical. Therefore, with assistance from TRAC–Monterey we created factor scores for each Factor and segmented the data sets in order to create a regression tree model for each of our Factors. We created training and testing data sets, training sets used 70% of the survey data to create the regression tree model and the remaining 30% of data was used in the testing set to validate. From these models we determined what the most important independent variables are in predicting Factor responses and used that to evaluate the effects of the Army's recruitment strategy in the Cyber Branch.

A factor score, according to Yong and Pearce (2013), is essentially an analyst-dependent measure that describes how they would score a factor. In our case, we first took the individual loadings of each factor and divided that by the sum of all loadings for that factor. For example one of the outputs for factor 1 score would be the loading factor for 21b, 0.401, divided by the sum all of all three loading factors above .400 for Factor 1 (0.401 + 0.791 + 0.763 = 1.955), which equals 0.205. This was done for each loading factor above 0.401. To calculate the factor score, the outputs for each loading factor were individually multiplied by the dataset of the variable that was associated with it and added to the rest of the loadings for that factor, illustrated in Figure 17:



```
w1sum<-0.401+0.791+0.763
w1.1<-0.401/w1sum
w2.1<-0.791/w1sum
w3.1<-0.763/w1sum
w2sum<-0.709+0.576+0.559
w1.2<-0.709/w2sum
w2.2<-0.576/w2sum
w3.2<-0.559/w2sum
w3sum<-0.664+0.659
w1.3<-0.664/w3sum
w2.3<-0.659/w3sum


data1$FactorScore1<-(w1.1*data1$X21A+w2.1*data1$X21B+w3.1*data1$X21C)
data1$FactorScore2<-(w1.2*data1$X20A+w2.2*data1$X20B+w3.2*data1$X20C)
data1$FactorScore3<-(w1.3*data1$X36A+w2.3*data1$X36B)
```

Figure 17. Factor Score Calculation Equations for 17A Survey Factors

Once we established the factor scores the conditions were set to create our regression tree analysis model. Before we set up the regression tree, we separated our data into two sets: training and testing. We created the regression trees in the training data sets and validated them in the testing set. For the purpose of relating these factors to the other variables in our survey and eventually facilitating the use of a regression tree models, they were correlated with seven other independent variables. The seven independent variables were: age, gender, rank, time in service (TIS), IT certifications, cyber experience (labeled “experience” in Figure 16) and operational/leadership experience (labeled “OP experience” in Figure 16). The independent variables for age, gender and TIS are self-explanatory and required no data manipulation for correlation. However, the independent variables for IT certifications, cyber experience and operational experience required us to sum up total instances for each respondent to create a total instances column for each independent variable and identify correlations from that column. For example, if respondent 13 had CISSP, CEH and SEC+ certifications, we created a column that identified respondent 13 as having three certifications and correlated that to the factors 1, 2 and 3. With all this in place we ran our regression tree model for Factor 1, job satisfaction, Figure 18, illustrates the results:

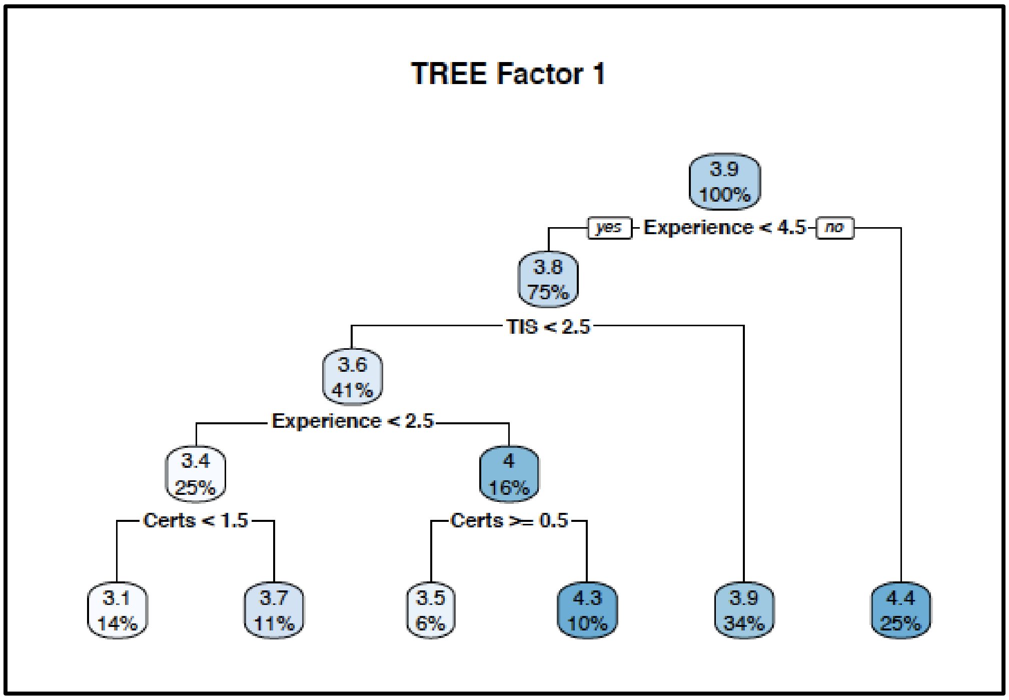


Figure 18. Regression Tree Model for Factor 1: Job Satisfaction

Figure 18 shows that based on our survey of 17As, the most important variable for determining job satisfaction was cyber experience. As explained previously, the input value for cyber experience is the sum of all experiences individually identified by the respondent. According to this model if respondents had 5 (rounded up from 4.5) or more cyber experiences (which was represented by 25% of the surveyed population) their job satisfaction score would be 4.4, which predicts that these individuals would at least agree (A) with variables 21a, 21b and 21c included in factor 1, job satisfaction. The next important factor in predicting job satisfaction was identified as TIS, the control variables or input values for TIS were:

- >1 year = 0
- 1–5 years = 1
- 6–10 years = 2
- 11–15 years = 3
- 16–20 years = 4
- Over 20 years = 5

This model deduces that if respondents had less than 5 cyber experiences but had at least six years TIS, their job satisfaction score would be 3.9 (which represents 34% of the surveyed population), predicting that they would lean more towards agreeing with variables 21a, 21b and 21c. After TIS the remaining branches of the regression tree drop significantly in population representation (from 75% and 34% to 41% and 10%). Of note, respondents who had less than five cyber experiences, less than six years TIS, and less than two certifications had the lowest job satisfaction scores and represented 14% of the survey population. The results of this model for Factor 1(job satisfaction) would suggest that achieving the recruitment goals for acquiring 17As with previous cyber experience, results in increasing the degree of job satisfaction. However, only 25% of the surveyed population met this criteria. This indicates that if the Cyber Branch is to have successful officers, then it must increase its emphasis in recruiting officers with more cyber experiences.

Next we ran our regression tree model for Factor 2 (assessment of the recruitment process) Figure 19 depicts the results:

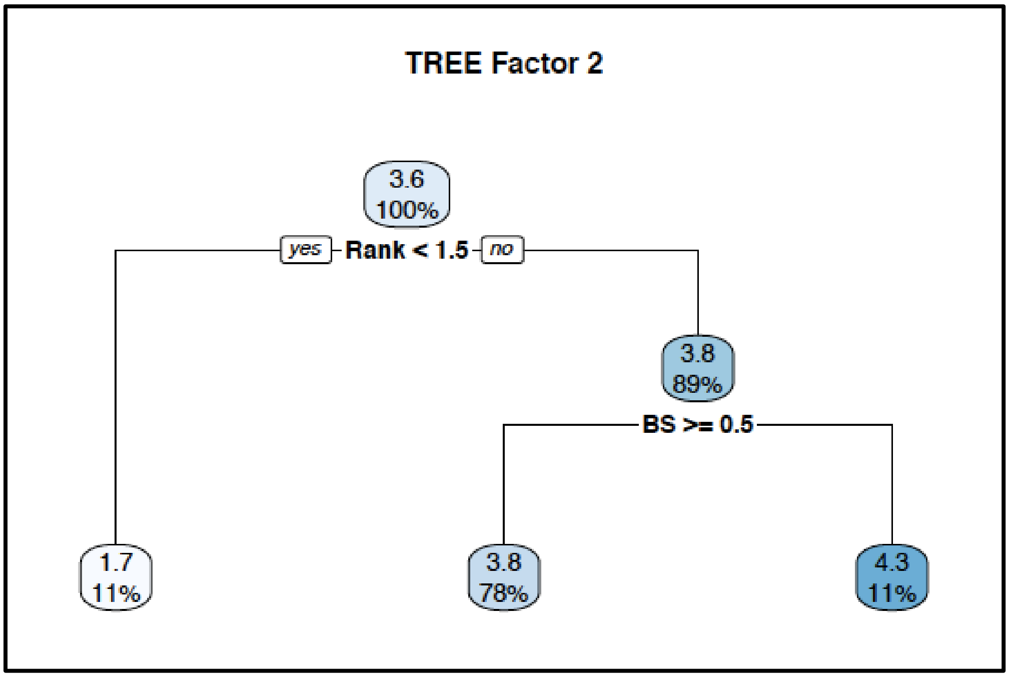


Figure 19. Regression Tree Model for Factor 2:
Assessment of the Recruitment Process.

According to this model, there are only two variables that determine the respondents' assessment of the recruitment process, the most important being rank. The input values for rank are:

- 2LT = 1
- 1LT = 2
- CPT = 3
- MAJ = 4
- LTC = 5
- COL = 6

Based on this regression tree if the respondent's rank was at least a 1LT (which represents 89% of the survey population) they would assess the recruitment process a score of 3.8, which is neutral to leaning to agree with variables 20a, 20b and 20c. The second variable that determines the respondent's assessment of the recruitment process is identified as the undergraduate BS degree. The regression tree model shows that if a respondent was at least a 1LT and had a BS, they would score the recruitment process a 3.8, while the respondents without a BS score it 4.3. The results of this regression tree model did not provide much distinction among respondents, and was both surprisingly positive and unanimous. However, we conducted additional analysis of respondents' assessment of the application/recruitment process that adds context to this determination, which we discuss later.

The last regression tree model we construct is for Factor 3 (Figure 19), motivation, which has five variables associated with it, but only two that load higher than .400 :

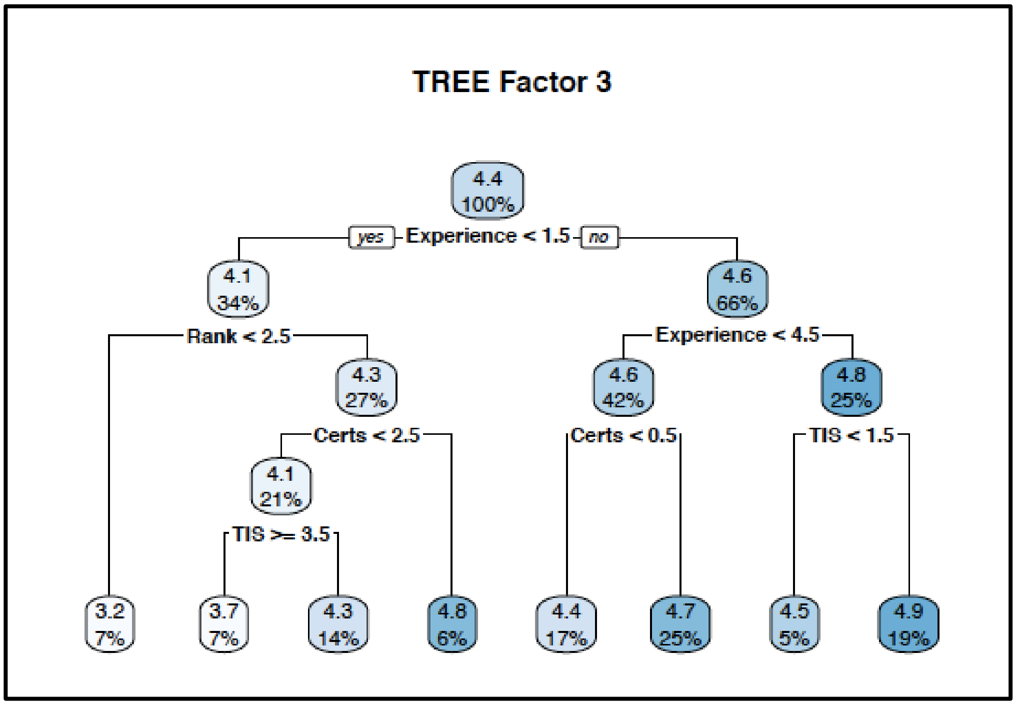


Figure 20. Regression Tree Model for Factor 3: Motivation

Figure 20 shows that based on this model, like factor 1, cyber experience is the most important variable for predicting respondents' motivation. According to this model if a respondent has two or more cyber experiences they will score a 4.6 in motivation, which is a leans toward strongly agree (SA), to variables 36a and 36b and is representative of

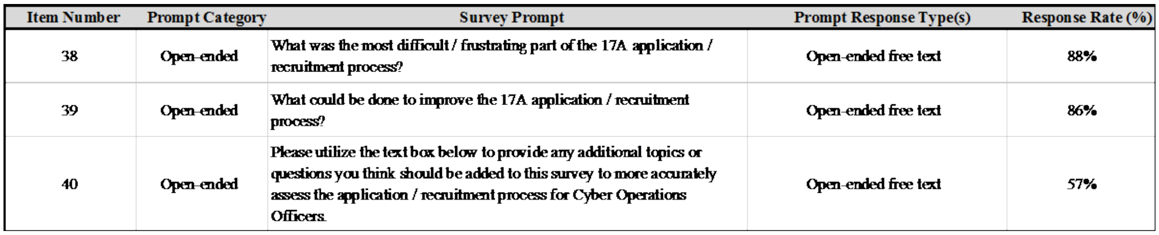
66% of the survey population. Following closely behind cyber experience in this models' level of importance in predicting respondent's motivation is rank. Based on this model if a respondent has less than two cyber experiences, but holds the rank of CPT or higher, they will score motivation 4.3, which is closer to agree, (A), for variables 36a and 36b and represents 34% of the survey population. Of particular interest in this model is that it goes down to the third tier of branches still representing 25% or more of the survey population. This gives relevance to the third tier branches of certifications and TIS in the prediction of respondents' motivation score. A respondent with less than two cyber experiences, in the rank of CPT or above and with three or more certifications will score motivation a 4.8, the second highest score in the model, which is strongly agree (SA) for variables 36a and 36b and represents 6% of the survey population. A respondent with between two to four cyber experiences and one or more certifications will score motivation a 4.7, which is strongly agree (SA) for variables 36a and 36b. Lastly, a respondent with five or more cyber experiences, with at least six years TIS will score motivation a 4.9, the highest motivation score in the model, which is strongly agree (SA) for variables 36a and 36b and represent 19% of the survey population. Of note, is that the lowest motivation scores are from respondents with less than two cyber experiences, and in the rank of 2LT or 1LT, representing 7% of the survey population. What this model suggests is that the recruitment goals achieved by the Army for acquiring 17As with cyber experience and certifications, in addition to demographic variables like rank and TIS, have enhanced the probability of Cyber Operations Officer's motivated by the mission of cyber and their ability to excel in the branch. However, only 19% of the survey population meet the criteria of achieving the highest score in the model. This is not necessarily a negative result because this model has multiple paths to relatively high motivation scores. According to this model 55% of the survey population meet the criteria for a 4.5 or above motivation score.

In summary, the regression tree models we created in our analysis predict that the recruitment goals identified by the Army can result in positive effects with regard to our proxy MOEs. However, these models also highlight that the current representation of each of the respective optimal effects is underwhelming. These predictions help in developing insight, but must be used with caution since the MOEs are subjective and require further research and corroboration for reliability.

b. Sentiment/Text Analysis

We continued our work with TRAC-Monterey and the "R" software package, specifically, R-TM: a text mining software package that uses "wordcloud," and "tidytext" to analyze text. As discussed in Chapter III, we decided to use only Questions 38 and 39 for analysis due to those questions having response rates above 80% (Table 14). Before conducting this analysis we removed common words like "the," "is," "of," "for"—commonly referred to as "stopwords"—that add no value to the analysis. Additionally, after initial screening, we removed words that were generically structural to the majority of responses, to include: technical, process, and branch. Lastly, we removed case sensitivity to ensure that words were not counted multiple times due to use of different cases. When constructing our survey we wanted to provide respondents with an opportunity to share their unfiltered thoughts on the Army's recruitment and selection process. Additionally, we wanted to have a catch-all that allowed respondents to highlight areas they felt were under-represented or not represented in the survey. While some responses were basic in nature, adding little, if any, value to our analysis, others laid thematic foundations that were echoed throughout our survey results for both the recruitment and selection processes. The primary purpose of this analysis was to add context to the MOPs and MOEs of the Army's recruitment strategy.

Table 14. 17A Survey Open-Ended Questions and Response Rates



Item Number	Prompt Category	Survey Prompt	Prompt Response Type(s)	Response Rate (%)
38	Open-ended	What was the most difficult / frustrating part of the 17A application / recruitment process?	Open-ended free text	88%
39	Open-ended	What could be done to improve the 17A application / recruitment process?	Open-ended free text	86%
40	Open-ended	Please utilize the text box below to provide any additional topics or questions you think should be added to this survey to more accurately assess the application / recruitment process for Cyber Operations Officers.	Open-ended free text	57%

We analyzed each question using the "recruitment related" and "selection related" categories, producing wordclouds (see Appendix F), graphical representations of frequently used words and some word correlations (see Appendix G). For each question and category we also identified common themes and provided quotes from respondents that captured these themes. For Question 38, which asks respondents about difficulties in the application/recruitment process, Figure 21 depicts the 15 most frequently used words for recruitment related responses:

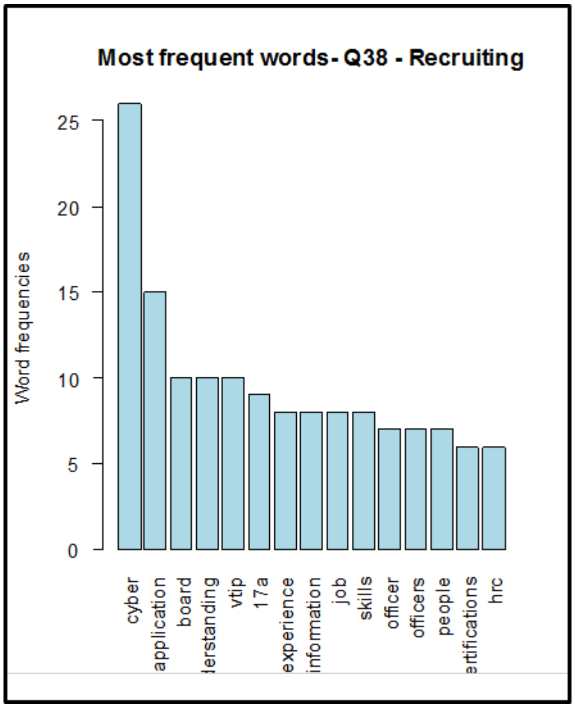


Figure 21. Most Frequently Used Words for 17A Survey Question 38, Recruitment-Related Responses

Our analysis showed that, in line with these frequently used terms, some of the common themes represented in these responses included:

a) Problems with the application/VTIP process, to include the submission process, assessment value and communications with HRC;

b) Understanding what the role of the cyber operations officer is, to include career path, job opportunities and duty descriptions; and

c) Understanding what the board was looking for in applicants.

Some of the recruitment related responses from the survey participants in regard to difficulties with the application/recruitment process are provided here:

a) Problems with the application/VTIP process:

- “The application process had no real way to effectively determine technical skills. The process relied heavily on self-reported information and certifications…”
- “Minute details led to me not being considered in the first VTIP (I sent an email asking whether I should submit my 4187 as a .tiff or .pdf file; did not receive a response; sent both formats; was disqualified because I sent a PDF file).”
- “Application does not adequately assess an individual’s qualification; application can be easily falsified to glorify an applicant”
- “The most frustrating part was formatting the documents to TIFF files.”

b) Understanding the role of the Cyber Operations Officer:

- “Uncertainty of branch’s future, unknown [Key Development] KD billets, unknown skills required and very non-transparent duty assignment methods.”
- “Non-defined paths to where I wanted to get where I wanted to work. Had to leverage personal relationships to find position that allowed me to do what I wanted in Cyber Branch.”
- “Lack of clarity over what a 17A actually does.”

c) Understanding what the board was looking for in applicants:

- “The lack of clarity for what the board was looking for in candidates was the most difficult part of the application…”

- “Figuring out exactly what they were looking for in a 17A. It seemed like there was a broad range of skills and experiences they were looking for that no one person could possess.”
- “There was not a lot of concrete information about requirements and expectations.”

For Question 38, selection related responses, Figure 22 depicts the most frequently used terms:

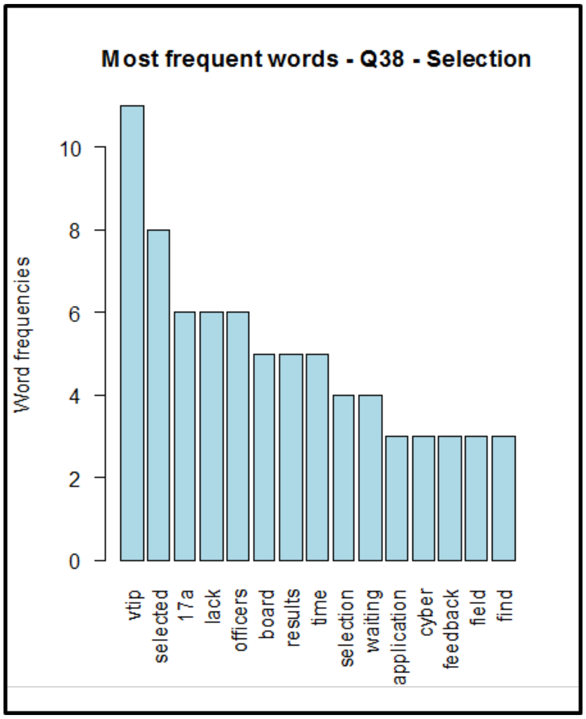


Figure 22. Most Frequently Used Words for 17A Survey Question 38, Selection-Related Responses

From our analysis of the selection related responses for Question 38, the common themes represented were:

a) Lack of transparency for the selection criteria and process, to include lack of feedback and/or guidance from HRC/Cyber Branch on selection;

b) Timeline for notification of selection; and

c) Validation of skill sets of selectees, to include observations of selected versus non-selected and flaws in VTIP based selection.

Below are selection related responses to Question 38:

a) Lack of transparency for the selection criteria and process

- "…Only frustrating was no feedback from the initial panel on why some were selected and some were not, i.e., what was weighted higher? STEM? experience on team? IT certs? Army OERs?"

- "The AAR from the first VTIP noted that a lot of officers not selected lacked 'passion' in their applications. With no guidance, it was hard for a lot of officers to write passionately in the few essay questions on the form."

- "Not receiving any feedback on selection criteria!"

b) Timeline for notification of selection:

- "The time it took to receive word on if I was accepted into the branch."

- "The timeline for the process changed and there was a significant amount of time before results were announced."

- "The wait to hear back!"

c) Validation of skill sets of selectees:

- "I'm seeing a lot of new 17As who lack any significant technical background, while I have already trained, qualified, and experienced 26A/26Bs who were turned down by the VTIP panel."

- "I've seen trained and qualified officers holding 17A positions who were not selected to VTIP into 17A, while I've seen new recruits into 17A who lacked even rudimentary technical skills."

- “The 17A program should require a rigorous assessment and qualification vs. a simple VTIP. VTIP does not equal vetting, and certainly does not ensure qualification.”

For question 39, which asks respondents how they would improve the application/recruitment process, Figure 23 illustrates the 15 most frequently used words for recruitment related responses:

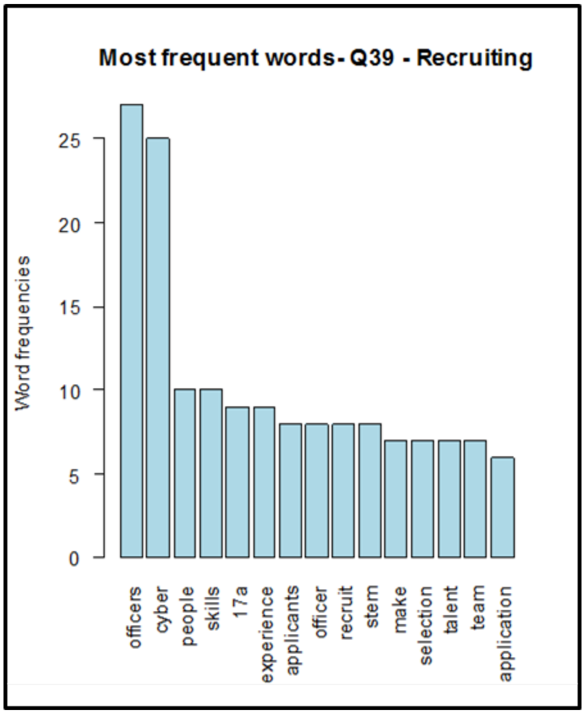


Figure 23. Most Frequently Used Words for 17A Survey Question 39, Recruitment-Related Responses

Based on our analysis, and in line with frequently used terms, the common themes among these recommendations for improvement were:

a) Expectation management, to include providing clear duty descriptions and skill requirements;

b) Expansion/reduction of the potential candidate/applicant pool, to include managing perceptions about who Cyber Branch is targeting for recruitment and who should be targeted. This recommendation had the unique distinction of having responses from both sides of the argument (expansion and reduction); and

c) Adopting a multi-dimensional recruitment approach, to include, training pipelines, mentorship programs and SME seminars.

Below are some of the actual "recruitment related" recommendations for improving the application/recruitment process from respondents:

a) Expectation management:

- "Provide feedback on desired attributes for 17As."
- "Continued socialization and general advocacy by cyber branch officials. Better expectation management regarding the overall selection process, criteria, etc."
- "I think a more concrete description of the expected degree of technical experience and expertise is necessary. I think it was unclear what amount was considered necessary, and what amount is considered desirable at each rank. Personally I believe both should be higher than the level demonstrated in the current selection process."

b) Expansion/reduction of the potential candidate/applicant pool:

- "Be open to a wider range of candidates. At first it seemed like this was just open for MI and SC officers. There is still a misconception about who the branch wants to recruit."
- "Recruit officers with leadership skills and technical skills; not just technical skills."
- "Recruit from hard STEM degrees (Computer Science, Computer Engineering, Electrical Engineering, and Mathematics)."

- "Continue to accept Officers from all Branches with STEM degrees; they offer a variety of insight, leadership, and technical ability that Officers fed directly into Cyber from Commissioning sources simply do not possess."
- "I'd argue that academic knowledge, while important, does not always make a good cyber officer. If we were to open the application process to accept more candidates and then vet the applicants in a qualification or assessment course (similar to selection to SF or CA), the I believe we would have much better results."

c) Multi-dimensional recruitment approach:

- "Leverage the current 17As to conduct installation and source of commissioning visits to conduct information briefings and Q&A sessions."
- "Provide cyber team members, team leads, and cyber staff members to discuss mission sets, training, expectations, etc., at virtual or in-person open houses."
- "Go visit Universities that have Scholarship for Service. There are 1000's of students that have to find government positions because of their scholarship. Why doesn't Army Cyber recruit at Carnegie Mellon University?"

For Question 39, selection related responses, Figure 24 displays the most frequently used terms:

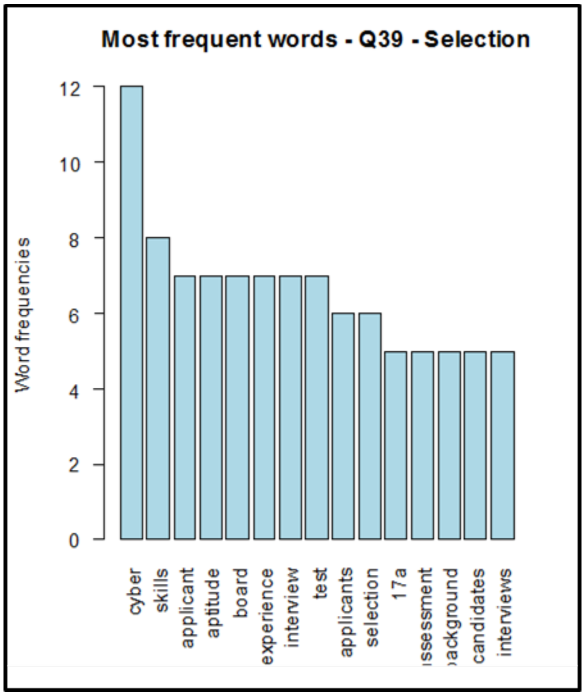


Figure 24. Most Frequently Used Words for 17A Survey Question 39, Selection-Related Responses

From the analysis of the selection related responses for Question 39, the common themes for improvements of the application/recruitment process were:

a) Aptitude testing/assessment, to include screening processes and technical testing;

b) Implementation of selection processes of other Army branches; and

c) Incorporation of the interview in the selection process.

Below are some of the actual responses that capture these themes:

a) Aptitude testing/assessment:

- "Perform some type of test/formal assessment that evaluates the baseline skills and capacity for technical learning of each officer."

- "A validated and verified test for skills and aptitude. Not just a test, but one that measures both independently. The Army has to very clear on what they want regarding type of skill, level of expertise in that skill and test for that. The same goes for aptitude."

- "Hold a week-long session where applicants have to take an active assessment to test their technical skills. Then progress to situations where applicants need to lead in a technical (and stressful) environment."

b) Implementation of selection processes of other Army branches:

- "Implement some form of technical assessment, ideally in a similar form as the Aviation flight exam…"

- "Use the Special Operations Forces model. Phase one = rigorous assessment (2-4 weeks in length). The assessment phase should be selective (50% or less selected. Phase two = qualification (18 months to 24 months). This phase should also have an attrition rate."

- "Recruit, like SOF. Do not just use VTIP process."

c) Incorporation of the interview in the selection process:

- "…After an initial application and screening based on technical background, there should be a technical interview to determine whether or not the person actually has the required background and skills."

- "Require personal interviews with each applicant. Don't weight STEM degree as much, focus on assessing cognitive aptitude."

- "There should be face-to-face (possibly over Skype) interviews, just as you would at a tech company. You cannot accurately evaluate technical leaders unless their skills are put to the test or are asked validation questions."

By analyzing these responses and identifying common usage of terms and themes, we were able to discern patterns that lead us to the following observations:

(1) Survey respondents were generally not happy with the Army's recruitment or selection processes for 17As.

(2) There is not a consensus among survey respondents on who should be targeted for recruitment by the Cyber Branch.

(3) Recommendations for improvements are generally in line with the DOD Cyber Workforce Strategy published in 2013.

Our analysis therefore provides relevant insight into the perception of the current 17A population regarding the recruitment and selection processes developed and implemented by the U.S. Army for Cyber Operations Officers. This allowed us to provide additional context to our evaluation of the effectiveness of the Army's recruitment strategy as well as its effects on the Cyber Branch as a whole.

C. "DID HIT" DATA—PDE RESULTS

The findings from the analysis of the data provided by PDE gave us our "did hit" data. These are the results, as reported by the Army, recruitment and selection processes for Cyber Operations Officers. The data is compared with the stated Cyber Operations Officer manning goals, survey data, and DOD and Army reported statistics from 2015. (DOD, 2015). Data on degree majors was not present in the data set. Analysis of the Army reported records for Cyber Operations Officers was used to do the following:

1. Validate the survey
2. Answer how well the Army is performing its tasks in 17A recruitment (MOPs)

D. PDE DATA ANALYSIS

As stated in Chapter III, analysis of the PDE data validates the survey data and provides a statistical description of the population of 17As as reported by the Army. Table 15 shows the rank proportions for survey respondents and as reported in the PDE Army Personnel Master database:

Table 15. Comparison of Rank Proportions for Survey Respondents and PDE 17A Population

Rank	Survey Response	% of Total Respondents	PDE	% of Total Population	Response % of Total Population
2LT	17	9%	36	10%	47%
1LT	22	11%	39	10%	56%
CPT	70	36%	128	34%	55%
MAJ	42	22%	119	32%	35%
LTC	32	21%	51	14%	63%
COL	9				

The survey had a 51% response rate, using the PDE reported number of 373 for the total number of 17As. Second lieutenants and majors are underrepresented in the survey respondent population. While first lieutenants, lieutenant colonels, and colonels are over represented in the same group. The response percentage, by rank, is 45% or greater for all ranks except for majors. The response rate for majors was deemed more than acceptable considering the size of the target population is relatively small.

Table 16 shows the gender proportions for the survey and as reported in the PDE database:

Table 16. Comparison of Gender Proportions for Survey Respondents and PDE 17A Population

	Survey		PDE 17A	
Gender	Number	% of Total Respondents	Number	% of Total Population
Male	171	89%	335	90%
Female	21	11%	38	10%

The proportions for males and females in both the survey respondent group and reported 17A demographics are within 1% of each other.

Finally, the age proportions, by rank, for both the survey and PDE database are listed in Table 17:

Table 17. Comparison of Age Proportions for Survey Respondents and PDE 17A Population

	Survey		PDE 17A	
Age Range	Number	% of Total Respondents	Number	% of Total Population
18-24	19	10%	34	9%
25-31	71	37%	105	28%
32-38	47	24%	134	36%
39-45	45	23%	83	22%
46+	10	5%	17	5%

The “25-31” age demographic is overrepresented in the survey respondent population by 8% percentage points in comparison to the Army reported proportion percentage. The “32-38” is underrepresented in the survey respondent population by 11% in comparison to the Army reported 17A proportion percentage. All other age range proportion percentages are within 1.5% of Army reported statistics for officers. Therefore, the high response rate and matching proportions suggest the results generalize the respondent information to the entire target population of 373 Cyber Operations officers, with respect to age.

Here is the comparison of Army recruitment goals, by rank proportion, with survey respondents, and the Army reported number from PDE:

Table 18. Comparison of Rank Proportions for Army 17A Recruitment Goals, Survey Respondents, and PDE 17A Population

Army Recruitment Goals for 17A		Survey Respondents		PDE 17A	
Rank	Proportion	Number	% of Total Respondents	Number	% of Total Population
2LT	26%	17	9%	36	10%
1LT		22	11%	39	10%
CPT	38%	70	36%	128	34%
MAJ	24%	42	22%	119	32%
LTC	12%	32	17%	51	14%
COL		9	5%		

The Army fell short of stated recruitment proportions for all ranks except for colonels and lieutenant colonels. The largest difference exists within the lieutenant population, with a shortfall of 6%. Recruitment of majors exceeded stated goal by 8%. The Army succeeded in acquiring 17As at field grade ranks and slightly underperformed with more senior company grade ranks. The cause of the underperformance for recruiting second and first lieutenants could be explained by the different process used for personnel acquisition for entry level officers. Unfortunately, data provided by PDE does not provide the variables necessary to ascertain the true cause of recruitment underperformance at those ranks.

1. Survey Validation

The data in the survey is validated by three statistics: survey response rate, rank proportions, and gender proportions. More than half of the entire 17A population, 192 of 373, responded to the survey. While the response rate was higher for senior officers, the response rates stratified by rank were all greater than 35%. Additionally, gender proportions for survey respondents and PDE were within 1% of each other. The high response rate and matching proportions for rank and gender suggest that the survey responses can be applied to the entire 17A population with reasonable accuracy.

2. Descriptive Statistics

Demographic information reported in the PDE database on the 17A population was compared against data reported from other armed services and Army wide statistics. Comparison of the PDE data with data reported by DOD and the Army illustrates the differences between armed services, Army level, and the 17A proportions for gender and race. This shows the unintentional impact that recruitment goals and the selection process has on the population of Cyber Operations Officers.

Here are the gender proportions for active duty officers, Army officers in grades O1-O6, and 17As in grades O1-O6:

Table 19. Comparison of DOD, Army, and 17A Gender Proportions

Gender	DOD Active Duty Officers	Army Officers	17A
Male	83%	82%	90%
Female	17%	18%	10%

Males are overrepresented in the 17A population by 8.09 percentage points in comparison to Army demographic statistics reported in 2015. (DOD, 2015). Females are underrepresented by the same amount in the target population. Females are overrepresented in Army Intelligence and Security Command (INSCOM) units, where they make up 19% of the assigned 17As. They exist at or below Army and 17A proportion levels in all other units. 17% of all Cyber Operations officers are assigned to INSCOM units. Appendix contains tables and graphs with descriptive statistics of the 17A population.

For race, the Army does not report "multi-racial." However, this is reported by the other armed services and is provided here for comparison. Table 20 lists the reported proportions for race and ethnicity in DOD, the Army, and as reported in the PDE database:

Table 20. Comparison of DOD, Army, and 17A Race Proportions

2015 Active Duty by Race		2015 Army Officers by Race	PDE 17A by Race
Race	% of Total	% of Total	% of Total
Asian	4%	5%	9%
American Indian or Alaska Native	1%	1%	1%
Black or African American	17%	13%	10%
Multi-Racial	3%		
Native Hawaiian or other Pacific Islander	1%	1%	0%
White	69%	74%	74%
Other/Unknown	4%	7%	6%

Black officers are underrepresented in the 17A population in comparison to both DOD and Army proportions. Asians are overrepresented by 3.55 percentage points above the Army reported percentage and 4.15 percentage points above the DOD proportion. Black officers are overrepresented in Army Network Enterprise Technology Command (NETCOM) units, where they make up 20% of assigned 17As. 28% of the 17As are assigned to NETCOM units.

3. MOP Summary—PDE

The Army stated goals for lieutenants and captains were not met. However, the Army exceeded the recruitment goals set forth for majors, lieutenant colonels, and colonels. It appears the process performs better on populations of officers with more established careers. The tools and mechanisms for recruiting entry level officers are significantly different. The recruiting environment and lack of competition with other organizations are not at play for officers in the rank of captain and above. More research would be required to determine why the 17A acquisition proportions increase with rank. Still, the Army was able to recruit within 23% of the stated goal proportion for lieutenants and within 11% of the stated goal for captains. The Army's recruitment process was a success for all ranks except for lieutenants.

E. SUMMARY

The Army reached an 89% achievement rate overall in "accomplishing tasks to standard" or achieving its targeted recruitment goals. There were only four of ten measured areas where they were UNSUCCESSFUL in reaching an 85% achievement rate of recruitment goals: target population; target attributes for operational/leadership experience and IT certifications; and target manning for LTs. As a result, we conclude that the Army was effective in creating an applicant pool of potential candidates for selection of 17As, however, based on some of the observed discrepancies by rank, we conclude that the selection process did not effectively differentiate between applicants in order to objectively select those with greater qualifications.

The regression tree models we created in our analysis predict that the recruitment goals identified by the Army can result in positive effects with regard to our proxy

MOEs. However, these models also highlight that the current representation of each of the respective optimal effects is underwhelming. These predictions help in developing insight, but must be used with caution since the MOEs are subjective and require further research and corroboration for reliability.

By conducting sentiment/text analysis we were able to identify common usage of terms and themes, and to discern patterns that lead us to the following observations:

(1) Survey respondents were generally not happy with the Army's recruitment or selection processes for 17As.

(2) There is not a consensus among survey respondents on who should be targeted for recruitment by the Cyber Branch.

(3) Recommendations for improvements are generally in line with the DOD Cyber Workforce Strategy published in 2013.

Our analysis therefore provides relevant insight into the perception of the current 17A population regarding the recruitment and selection processes developed and implemented by the U.S. Army for Cyber Operations Officers. This allowed us to provide additional context to our evaluation of the effectiveness of the Army's recruitment strategy as well as its effects on the Cyber Branch as a whole.

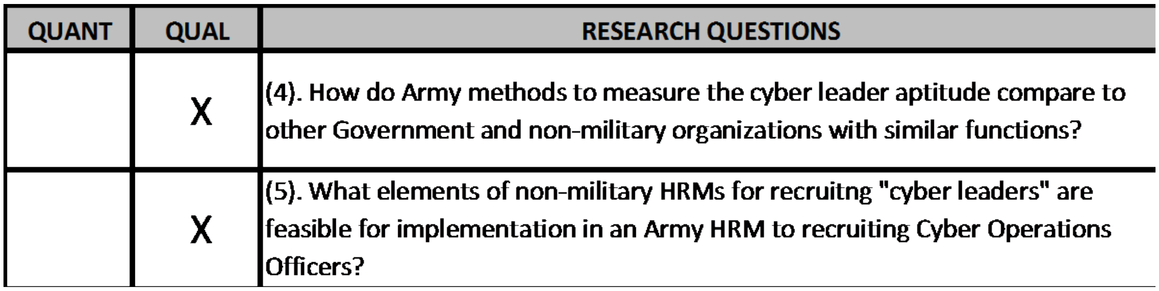
Analysis of the PDE data set was used to validate the survey and determine applicability to the 17A population. With response rates of over 45% for all ranks except for MAJs (35%), we determined the survey was representative of the total target population. Descriptive analysis of the PDE data set highlights some deviations in the 17A race and gender proportions from reported Army averages.

V. COMPARATIVE ANALYSIS

A. INTRODUCTION

To measure the effectiveness of the Army's recruitment processes used to select the initial population of Cyber Operations officers, a comparative analysis with other military, governmental, and non-governmental organizations was conducted. Documentation on the recruitment practices for Google, Facebook, Department of Homeland Security (DHS), and special branches within the Army are used. The comparison analysis was used to answer these research questions:

Table 21. Research Questions Addressed by Other Government and Non-government Organizations



QUANT	QUAL	RESEARCH QUESTIONS
	X	(4). How do Army methods to measure the cyber leader aptitude compare to other Government and non-military organizations with similar functions?
	X	(5). What elements of non-military HRMs for recruitng "cyber leaders" are feasible for implementation in an Army HRM to recruiting Cyber Operations Officers?

This section will focus on three areas: recruiting environment, recruitment pool development, and selection processes. We compare the HRM constructs, models, and frameworks used by the selected organizations. Based on the case study of Google's recruiting practices (Sullivan, 2005), the Federal Cybersecurity Workforce Strategy (Office of Management and Budget [OMB], 2016), and the legislative acts and DOD directives, we categorize the models used by the three types of organizations. First, we describe the factors which impact the environment in which the organizations recruit. The legal authorities coupled with the form and function of companies inform their recruitment strategies. For example, the military is not a for-profit organizations. Since the transition to the AVF in 1973, the Army, along with the other services, must compete with the rest of the federal government and civilian organizations for labor (Carter, P., Kidder, K., Schafer, A., & Swick, S., 2017). The way in which personnel are used, even for equivalent skill sets, determines how those personnel are recruited and selected. Second, we identify the criteria and attributes the selected organizations use to create recruitment pools. Recruitment pools are the individuals in the labor population that possess the desired skills, education, experience, and industry credentials. These are the attributes that directly support organizational IT functions and accomplishment of strategic goals. We describe the tools used by the selected organizations to identify personnel with the targeted attributes and to assess their level of mastery. Third, our research compares selection processes between the aforementioned organizations. Selection processes are the mechanisms and tools private companies and government entities use to approve or deny employment to personnel in the recruitment pool.

B. GOOGLE

In *A Case Study of Google Recruiting*, Dr. Sullivan identifies how Google's views on labor are transformed into a recruiting tool. (Sullivan, 2005). The focus on employee satisfaction and commitment places Google closer to the "soft" end of the spectrum. (Storey, 1989). The company uses a concept called "20% time" to attract some of the best and brightest in IT (Sullivan, 2005). "20% time" is loosely defined as a program which allows employees to spend 20 percent of their time working of projects of their own choosing (Sullivan, 2005). Numerous articles about "20% time" debate the effectiveness of the programs as a recruiting tool versus the benefits of the program in practice, to mixed reviews. In addition to "20% time," Google goes to great lengths to gain employee commitment. Job satisfaction and comfortable work environment are touted ahead of compensation, which is impressive considering initial salary offerings from Google are well above the industry norm (Sullivan, 2005).

1. Recruiting Environment

Google is a private, for-profit company. As such, offensive cyber activities are considered criminal, when conducted against another private entity, and acts of war when conducted against another nation, without the authority of the United States federal government (Crootof, 2012). As a private organization, Google is limited to defensive cyber activities. Therefore, Google has to recruit personnel with capabilities based on these legal constraints. It is here the qualities of the Guest model align with Google’s recruiting strategy (Guest, 1987). The focus on recruitment operations, and more importantly, prioritizing resources to recruitment operations, allows Google to obtain quality talent in such large volume. (Sullivan, 2005). Google’s policies focus on the first and third sub-dimensions of the Guest model, quality of staff and public image, more (Guest, 1987). However, the path to the second sub-dimension for Google, quality of performance, travels a more circuitous route. Performance is achieved through an organizational strategy that uses recruitment as a center of gravity (Sullivan, 2005). Google’s institutional performance is built on attracting top performers. The first and third sub-dimensions are used as a means to achieve the second sub-dimension. The positive public image generated by quality of performance, due to high quality staff, is then recycled back into recruitment efforts. Because the company views its human capital as an asset, Google expends much effort on building a culture of employee commitment (Sullivan, 2005).

2. Recruitment Pool Development

Six job announcements for cybersecurity positions from Google’s “Google Careers” website were analyzed to determine how Google develops recruitment pools. None of the positions entailed supervisory duties and all of the positions are with Google and not a contractor or sub-contractor. Here are the job titles for the positions reviewed:

a) Network Security Engineer

b) Security Engineer, Forensics

c) Security Engineer, Information Security Assurance/Red Team

d) Security Engineer, Detection

e) Security Operations Engineer, Google Cloud

f) Software Engineer, Security

Advertised job openings can be filtered by role, division, education, experience, and type. Type is defined as part-time or full-time employment, temporary work, or internship (Google, 2017). Division differentiates between the various companies under the Google umbrella. For example, YouTube and Google Fiber are listed under the division filter. Salary is not mentioned in any of Google's job announcements. Following a brief description of the position are lists of the responsibilities and qualification requirements. Qualifications are subcategorized as minimum and preferred. All of the positions listed a bachelor of science (BS) degree as a minimum requirement. Two of the positions listed experience with vendor specific software as a minimum qualification. For preferred qualifications, all of the job announcements listed experience with narrow wording. The specificity of the experience could only be obtained through an IT certification and work which required an IT certification. For example, the network security engineer announcement lists "experience with JunOS and Cisco IOS/XR security features" as a preferred qualification. Not only would a prospective hire need to possess a certification for Juniper and Cisco devices, he or she would also need work experience with that equipment.

3. Selection Process

Google focuses many of its organizational resources on recruitment and selection of personnel. The primary mechanism for selection is the interview. An iterative behavioral interview process is used to observe and gauge a candidate's reaction in cybersecurity scenarios familiar to Google. This is where Google applies its huge data analysis resources to ensure the behavioral interviews actually predict possession of desired attributes (Sullivan, 2005). A significant emphasis is placed on cultural fit and talent.

C. FACEBOOK

1. Recruiting Environment

Facebook faces the same set of circumstances as Google in the recruiting environment. As a for-profit company, it is bound by the same laws, which restrict cyber activities to the defensive operations. This places Facebook in direct competition with

Google and every other for-profit company with similar personnel needs. Facing fierce competition in a very limited labor pool, the company has taken a holistic approach to achieve employee commitment. Facebook uses three approaches to attract exceptional talent: look for builders, background diversity, and cultural fit (Feloni, 2016). The experience of the interview and selection process is used to sell candidates on organizational philosophy and core values. From this perspective, Facebook borrows elements from two "soft" HRM models, Guest and Storey, to recruit talented cybersecurity professionals. An organizational philosophy based on core values underpins the recruitment policies. These five core values inform the method in which the organization recruits (Feloni, 2016):

- Boldness
- Impact
- Move fast and break things
- Openness
- Build social value

The core values focus on contributions from the employee perspective. This directly maps to two sub-dimensions of the Guest model, quality of performance and public image. The offer of opportunities and organizational culture are the primary means by which Facebook separates itself from other companies in the recruiting environment.

2. Recruiting Pool Development

Six job announcements were reviewed for cybersecurity positions from Facebook's "Facebook Careers" website (Facebook, 2017). Almost all supervisory and high skill positions at Facebook are Facebook employees. Many of the non-supervisory positions, moderately and low skilled, are contractors. Here are the job titles for the positions reviewed:

- Technical Program Manager, Infrastructure Security
- Technical InfoSec Compliance Analyst

- Manufacturing InfoSec Engineer
- Security Engineer—Online Safety and Security
- Malware Researcher
- Security Engineer—Detection Infrastructure

Salary is not mentioned in any of the Facebook job announcements. Qualifications for the job announcements are separated into two sections: minimum qualifications and preferred qualifications (Facebook, 2017). The number of minimum qualifications ranges from 3–13. Three of the six positions have a list of preferred qualifications. Four of the six positions require a bachelor's or master's degree in computer science or STEM field. Two of the positions mention IT certifications as a minimum requirement. All of the positions require the ability to work in teams (Facebook, 2017). Five of the six positions prefer applicants to show contributions to their respective fields in the form of blogposts or other published work. It appears that Facebook uses formal education and participation within the cybersecurity communities of practice as discriminators for recruitment. The ability to work as a member of a team is important. However, only the Technical Program Manager job announcement mentions leadership experience as a desired quality. Emotive words such as "passion," "love," and "motivation," appear several times in each job announcement. In addition to a display of work in their respective fields, applicants must demonstrate a commitment to their craft as well. Due to the legal authorities under which Facebook operates, all of the positions focus on defensive cyber activities. A theme of protection of corporate assets and users is prevalent throughout the position descriptions. The ability to convey the impact of cybersecurity on other aspects of the organization or business functions appears in five of the six job announcements.

Based on the review of the job announcements, Facebook casts a wide net. There are not a lot of hard requirements. For example, "knowledge of spam and instant messaging attacks" lacks specificity in comparison to requirements in government and military organizations. This could be an indicator of the fluidity of positions that characterize the private company work environment. Creating such a large pool to select from shifts the burden from recruitment to the selection process. Facebook appears to focus on formal education, industry experience, and fit. The focus on industry experience is different from work experience in this context. A self-motivated individual is capable of making contributions in the field of cybersecurity without working in cybersecurity. This shows Facebook’s willingness to look at applicants outside the cybersecurity industry, but who may have an aptitude for the work.

3. Selection Process

From the recruitment pool, Facebook, like most private companies, uses interviews as the primary method of selecting cybersecurity personnel. What sets Facebook apart is the use of iterative interviews with both behavioral and situational questions (Feloni, 2016). Each interview may focus on different selection criteria which range from experience to cultural fit. For example, the first interview would be conducted with someone in the Human Resources (HR) department. However, subsequent interviews involve employees in the department a candidate may work with or other departments the candidate may interact with. The interviewer observes reactions and behaviors to assess both capability and fitness for Facebook. In contrast to Google and its cohort of recruiters, Facebook relies on observation of candidates within its corporate environment to make the final selection.

D. DEPARTMENT OF HOMELAND SECURITY

1. Recruiting Environment

The HRM construct for a non-military governmental agency such as DHS consists of both “hard” and “soft” elements. This is due to both the function of the organization and the legal authorities under which it operates. Title 6 of U.S. code, domestic security, establishes the mission of DHS as the “prevention of terrorist attacks within the United States; minimize the damage, and assist in the recovery from terrorist attacks that occur within the United States; crisis response and emergency planning; ensure the functions of DHS; ensure economic security; monitor and sever connections between illegal drug trafficking and terrorism; and ensure the civil rights and civil liberties are not diminished by efforts aimed at securing the homeland” (U.S., 2005). As a government entity, there is an emphasis on stewardship of public funds. This leads to tighter control of activities within DHS. Recruitment of federal workers is standardized by OPM. The manner in which DHS, and other federal agencies, recruits is directed by an external organization. However, who DHS recruits is an internal decision (OPM, 2017).

Chapter 6 of U.S. code Title 6 covers the cybersecurity guidelines for DHS. The Federal Cybersecurity Workforce Strategy provides more detailed guidance on the recruitment of highly skilled personnel to support DHS functions (OPM, 2016b). Salaries and compensation are tightly controlled by law. To compensate for this restriction, federal workers receive more secure benefits packages (OPM, 2017). For example, healthcare packages and pensions for federal workers offer better security than their non-governmental counterparts. This allows DHS to compete on somewhat equal footing with private companies that offer significantly higher salaries, but less job security. We view that this depressed salary scale of federal workers leans more toward “hard” HRM constructs. Similar to private companies, DHS uses the culture of its work environment to recruit. DHS provides the opportunity of public service, something few private companies can offer (DHS, 2017). Employee commitment has to be high to attract skilled labor for comparably low costs. This creates a friction point within the Storey construct where “hard” and “soft” aspects exist within the same organization due constraints born from legal restrictions and institutional function.

DHS has dealings with both the private sector and national defense. Coordination with for-profit companies is crucial to the protection of domestic infrastructure. DHS must understand the motivations of these companies and the industries in which they operate. Naturally, cultural aspects of the larger cybersecurity community shape the cybersecurity community in the federal government. Also, habitual relationships have formed between DHS and the armed services as enemies set their sights on targets within the United States. In this respect, DHS has become a translator of sorts. The federal agency has learned to discuss cybersecurity in both the language of private companies and national defense community. As a government entity, DHS is more susceptible to the political environment than a private company (Fombrun et al., 1984). It has had to implant aspects of “soft” models, specifically recruitment of high quality people based on a culture of service, to accomplish the mission set forth in Title 6 (U.S., 2005).

2. Recruitment Pool Development

As previously explained in Chapter II, federal agencies develop position descriptions in accordance with OPM regulations (OPM, 2017). Five job announcements and two position descriptions for DHS were analyzed comparison purposes. The position description is a detailed breakdown of a position within a federal agency that accompanies a formal request to advertise said position on USAJOBS.gov (OPM, 2017). OPM uses the information contained the position description to create a job announcement on their website (OPM, 2017). Both the position descriptions and job announcements are for IT management series 2210 positions. 2210 series covers "two-grade interval administrative positions that manage, supervise, lead, administer, develop, deliver, and support IT systems and services. This series covers only those positions for which the paramount requirement is knowledge of IT principles, concepts, and methods; e.g., data storage, software applications, networking." The security subsets of the 2210 series, INFOSEC, are the positions that we focused on for this research (OPM, 2011). The position descriptions are both for INFOSEC with pay grades of GS-15. (OPM, 2017). Here are the position titles for DHS job announcements:

- IT Project Manager
- Four (4) IT Specialist (INFOSEC)

The pay grades range from GS-09 to GS-14. Salaries for each position are given in ranges based on the pay grades, from $65K to over $145K per year. The job announcements, outside of pay grade and position title, provided very little information about the positions in comparison to the position descriptions provided by DHS. Where the position is located and some general description of duties is the only additional information given. It is less obvious to applicants whether they possess the required skills for a given position. Filtering the pool of qualifying candidates is automated based on the requirements included in the position description from DHS.

The position descriptions provide both detailed account of duties and specific tasks required of the position. Over nine of the 16 pages in both documents outline the major duties and specific tasks. Noticeably absent are education requirements beyond a high school diploma. It can be inferred that to possess the knowledge, skills, and abilities (KSA) listed, an applicant had to complete some level of formal education or training after high school (OPM, 2017). For federal jobs, work experience can be substituted for formal education. However, that is determined during the selection process, not the recruitment process (OPM, 2017). For example, under "Knowledge Required by Position," an applicant must have the following:

- Expert knowledge of IT security principles and related disciplines
- Comprehensive knowledge of system and network operating systems and architecture
- Extensive knowledge of national and international security policies and technical practices governing the installation, maintenance, and operation of sensitive and classified data systems.

The acquisition of these KSAs requires some formal education, training, or both. OPM uses automated tools to filter applicants and develop a recruitment pool based specific criteria (OPM, 2017). Because the system creating the recruitment pool has this knowledge and not the applicant, more people, qualified and unqualified, will apply for the position. As in the Guest model, DHS uses its culture of public service to recruit (Guest, 1987). Specifically appealing to applicant's sense of patriotism, which maps to the public image sub-dimension, OPM uses "nation," "American," and "purpose" to signal cultural benefits of employment at DHS. This is done to attract cybersecurity professionals who prioritize job security and benefits over pay. The lack of detailed information in the job announcement is done to attract as many applicants as possible. Aspects of the Harvard model also appear in OPM and DHS recruitment practices. The federal hiring process is not rapid. It can take up to six months to fully bring an employee onto the job (OPM, 2017). Once a federal employee completes their probationary period and is fully hired, that individual typically does not leave the organization for some time (OPM, 2017). Therefore, OPM and DHS HRM policies have to take a long strategic view because federal employees are hired to against a function. Compared to private companies where strategic goals are significantly impacted by the economic environment and technological transitions, the federal government seeks stability to maintain consistent outcomes. Volume recruiting appears to be the preferred method for ensuring a steady flow of highly skilled labor into DHS.

3. Selection Process

At DHS, the hiring process is more prescribed and regimented to ensure fairness and compliance with applicable laws or regulations. OPM provides the hiring process analysis tool, which is a "timeline tool is based on a generic process model for conducting efficient, high-quality hiring" (OPM, 2017). Below are the three steps of the hiring process analysis tool:

- Explore the steps in the OPM hiring process model and recommended days for completing each step.
- Determine the number of days the hiring agency will take to complete each step. Prioritization is also done in the second step.
- Identify how the hiring agency's process may deviate from the OPM hiring process model.

Special care is taken to document all actions taken during the hiring process. It is during the fourth step of the OPM hiring process model that KSAs are developed, methods to assess KSAs (interviews, tests, etc.) are identified, and a ranking system is developed (OPM, 2017). The number and types of interviews are documented before the position is announced. All applicants must undergo the same interview and assessment process unless circumstances dictate otherwise. For example, an applicant with a disability may need to undergo assessment testing at an alternative location (OPM, 2017). Overall, the DHS selection process has to find qualified candidates with the best fit bounded by a system focused on fairness and equality.

E. COMPARATIVE ANALYSIS OF ARMY CYBER OPERATIONS OFFICER RECRUITMENT PROCESSES

1. The Storey Model

a. The Army HRM

To compare the Army's officer recruitment processes, it is helpful to identify where each organization exists on the scale between "soft" and "hard" human resource management (HRM) constructs (Storey, 1989). The authorities under which DOD and the armed services operate significantly impact how those organizations behave in the recruitment environment. The "up or out" officer system established by the Defense Officer Personnel Management Act (DOPMA) created a human resource environment based on steady influx of guaranteed labor and time based promotions (Defense Officer Personnel Management Act [DOPMA], 1980). Labor population is controlled primarily through promotion rates. The transition to the all-volunteer force nearly 40 years ago decreased the certainty in the influx of skilled labor. Improving civilian opportunities increased competition between the Army and private organizations for top talent. To keep pace, the Army had to adopt some "soft" HRM approaches to attract personnel with the skills required of Soldiers on a battlefield that is more reliant on technological advances (Carter, Kidder, Schafer & Swlck, 2017). Eventually, DOD and the Army could not keep pace with the financial packages offered by private companies for specialized skill sets with both military and civilian applications. This led to focused advertising campaigns extolling the prestige and purpose that accompanies military service. Employee commitment crept up the prioritization ladder and forced the Army to incorporate some elements of "soft" HRM constructs. Figure 25 illustrates where we assess that the Army lies on the line between "soft" and "hard" constructs, in relation to the other organizations we studied.

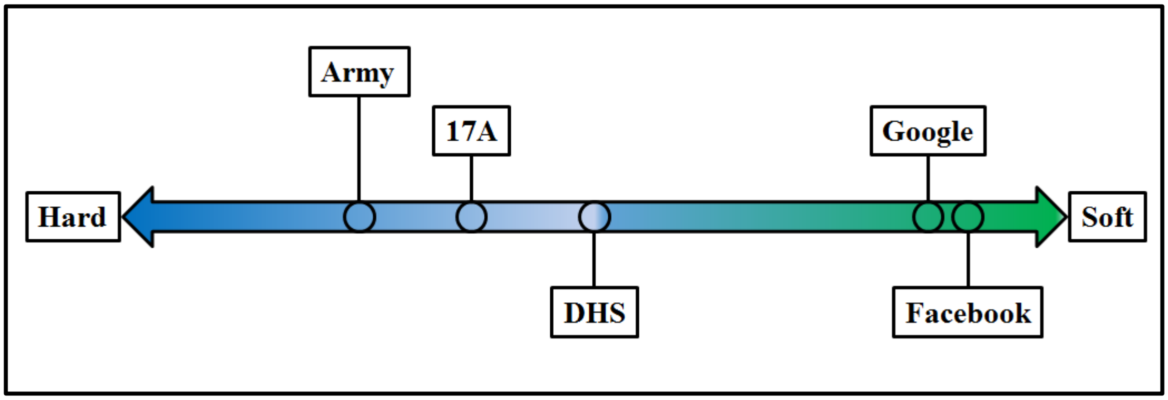


Figure 25. HRM Model Comparison Spectrum

We assess the recruitment of Army Cyber Operations Officers prioritizes employee commitment more than other Army occupational specialties due to the high level of competition with other organizations. The first sub-dimension of the Guest model, quality of staff, underpins the approach to recruiting from the existing officer population. Becoming a 17A provides Soldiers the opportunity to learn and display, in their opinion, underutilized skills. The Army appeals to the target populations sense of professional pride to attract applicants. To a lesser degree the second sub-dimension of the Guest model, quality of performance, is used in the recruitment process. Army Cyber Branch presents officers with a chance to work with some of the best cybersecurity professionals in the Army and DOD. While there is more focus on individual commitment for 17As, the context in which their duties are performed push the HRM construct toward the "hard" end of the spectrum.

2. Other Army Specialty Recruitment Processes

The Army used the standard process of submitting requirements to U.S. Army Recruiting Command (USAREC), the organization responsible for recruitment and selection. However, we suggest that compared to other Army branches that require specialized recruitment processes for personnel acquisition, Cyber branch does not use all available tools for recruitment pool development and selection. Aviation and Special Forces Branches utilize combinations of mental and physical assessments to determine candidates' aptitude for success in their respective fields. The recruitment of Cyber

Operations officers relies heavily on civilian education, industry certifications, and experience for recruitment and selection.

a. Psychometric Screening

Army Aviation Branch utilizes the Flight Aptitude Selection Test (FAST) to assess candidates' aptitude to operating rotary wing aircraft under the unique environments and circumstances of combat. Rigorous physical assessments are required as well to provide USAREC and Aviation branch with a more holistic view of personnel. Because Aviation has civilian applications, the military aviation workforce framework is informed by a combination of best business practices, laws, and lessons learned. Army Special Forces goes a step further, utilizing psychometric testing to add another layer of information on the assessment of candidate's aptitude. Psychometric assessments illustrate how the interactions between behavior and skill may affect performance in certain roles (Patrichi, 2015). Considering the criticality of the roles that both Aviation and Special Forces play in the overall DOD set of capabilities, it seems prudent that additional resources would be implemented to assess aptitude.

As previously stated, the Army Cyber Institute (ACI) determined that traditional methods for officer accessions are not conducive to accurate assessments of cyber aptitude (Morris and Waage, 2015). Because of this gap in assessment capability, the Air Force led the development of the Armed Services Vocational Aptitude Battery-Cyber Test (ASVAB-CT) (Trippe et al., 2014). While this test focuses more on entry-level cyber occupations, it could give some indication of future performance for lieutenants. The System Administrator, Audit, Network, and Security-Cyber Talent Enhanced (SANS-CTE) test, piloted by the Army, provides an improved assessment of cyber skills (Morris and Wage, 2015). However, the Army uses neither test in the recruitment of Cyber Operations officers. Given the non-traditional cognitive problem solving requirements of operating in both physical and logical space, it would also seem prudent for Cyber branch to administer some form of psychometric testing as well.

b. Non-Standard Accessions

Within the Judge Advocate General Corps (JAGC) and medical occupational specialties, there are mechanisms for recruitment at levels higher than entry-level. Aviation and Special Forces Branches prioritize field experience due to the emphasis on operations in combat environments. This leads to a long development program after aptitude assessment to create a workforce that possesses the requisite skill sets. In contrast, JAGC and medical professionals in the Army are educated and trained at civilian institutions. Personnel are "painted green" through indoctrination training to apply their civilian training in an Army context. Because qualification leans decidedly more on credentials from external organizations, the Army created processes to hire candidates at ranks higher than lieutenant (Department of the Army [DA], 1994). This allows for the commissioning of officers with highly technical or specialized skills in fields where military experience is obtained through means other than time in service. This shifts the burden of physical assessment and readiness to the indoctrination program. As with JAGC and medical professionals in the Army, a separate promotion system was developed to accommodate the non-standard commissioning process.

Cyber branch should consider adopting a non-standard commissioning process to acquire personnel with more civilian education and industry credentials. However, the development of a different promotion model could cause some cultural friction between 17As and the rest of the officer corps. Adaptation of established mechanisms from the Chaplain Corps, JAGC, and Army medical community would make the transition somewhat smoother than creating a promotion system from scratch. One of the advantages to recruiting officers at ranks higher than entry-level is the creation of a larger recruitment pool. This would put the Army in direct competition with other governmental agencies and non-military organizations for cybersecurity talent, the same as JAGC and the medical occupational specialties. Mature and established non-standard commissioning processes exist within the Army. Cyber branch might use these tools, in conjunction with others, to create a robust cybersecurity workforce that meets strategic needs.

c. Interview Processes

Current Army Cyber Operations officer recruitment processes acquire personnel using two methods: entry-level recruitment through the Reserve Officer Training Corps (ROTC) and from the existing officer population through the Volunteer Transfer Incentive Program (VTIP). Cyber branch and unit commanders in the Army have to accept the officers provided by Human Resources Command (HRC). An interview process, utilized by DHS, Facebook, and Google, would provide a better assessment for both targeted attributes and organizational fit. The interview process also affords unit commanders the right to refuse personnel that may possess the level of education and industry credentials, but lack fitness of personality traits for particular roles. For example, a field grade Cyber Operations officer has the education and certifications to become a member of a cyber protection team. Through an interview process it is learned that officer is better suited for work in an operational headquarters. Feedback from the process would be used to place the officer in position to perform better and identify areas to improve upon. This would represent a significant shift towards softer HRM models where the feudal nature of Army major commands (MAJCOM) is accounted for. The interview process processes prioritize cultural fit and technical proficiency equally.

One of the criteria Facebook uses to develop its recruitment pool is candidate contribution to cyber community. There is some information sharing within the Army cybersecurity community, but it is limited to past and present Army officers. To encourage innovation and dialogue, Cyber Operations officers should actively participate in non-military cybersecurity community. Granted, much of the work performed by 17As exists at the classification of secret or higher. However, discussion of the underlying principles and methods are valuable to the industry at large. Establishing this relationship with the community of practice could also ease the transition for officers commissioned at ranks higher than lieutenant, if the Army chose to go that route. Cybersecurity professionals would be more familiar with information security concepts in the Army context because of frequent interactions. Most importantly, contributions to the industry act as a recruitment tool to attract talent looking for different opportunities to employ their skills.

Table 18 illustrates the tools the abovementioned organizations use to select candidates from their respective recruitment pools.

Table 22. Selection Tools

	Google & Facebook	DHS	Army	17A
Aptitude Testing			✓	
Psychometric Testing			✓	
Interview Process	✓	✓		
Right of Refusal	✓	✓		
Mid-Career Accessions	✓	✓	✓	

F. SUMMARY

The recruitment of cybersecurity professionals is informed primarily by the recruiting environment, how the recruitment pool is developed, and personnel selection processes. Organizational function and authority shape the work roles those professionals occupy. Private companies are prohibited from engaging in offensive cyber operations due to legal implications. However, offensive and defensive cyber operations required similar sets of skills, education, and experience. Due to the abnormally low unemployment rate and limited number of candidates who possess the desired cyber security attributes, Facebook and Google expend a large amount of resources on recruitment. By comparison, DHS and the Army possess the authority to conduct offensive operations, but recruit cybersecurity personnel under more constraints. All of the organizations reviewed use a combination of tools to assess aptitude and organizational fit commensurate with their respective functions. Civilian organizations lean more heavily on interview processes for assessments. The Army uses aptitude and psychometric testing for specialty recruitment. Despite the convergence by all of these organizations on similar desired attributes, the differences in recruiting environments significantly impacts how cybersecurity professionals are acquired.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS AND RECOMMENDATIONS

The purpose of this research was to evaluate the HRM model used by the U.S. Army for the recruitment of Cyber Operations Officers to assess its effectiveness and to examine the effects of its continued use. In this chapter we answer our research questions identified in Chapter I, detail the practical implications and limitations of our research, and provide recommendations for further research on this topic.

A. RESEARCH QUESTIONS

1. Technical Skill Set Requirements

Our primary research question asks, “How does the Army’s HRM for recruiting Cyber Operations Officers account for the technical skill set required to lead cyber forces?” Based on our research it is clear, the Army uses cyber experience, STEM degrees and to a lesser extent IT certifications to account for the technical skill set required. However, there is evidence that accounting for this skill set varies based on rank.

2. Manning Requirements vs. Individual Requirements

Our second research question asks, “How does the Army’s recruitment strategy for Cyber Operations Officers balance manning requirements and individual capability requirements?” Based on targeted attributes the Army used to create the recruitment pool for the first two iterations of the 17A VTIP, the researchers conclude the recruitment process focused decidedly on organizational manning requirements. This was especially evident for field grade ranks, where a premium was placed on leadership and operational experience over technical proficiency and credentials. The primary discriminators for officers eligible to participate in the VTIP were rank, education, and certifications. These discriminators were used to create a force structure based on rank proportions. The lack of granularity for desired attributes which could be used to identify fitness for any of the cyber mission subsets (defense, attack, exploitation, and policy) illustrates prioritization of the organization over the individual. This also led us to conclude that while the Army has incorporated elements of ‘soft’ HRM constructs to remain competitive in the labor market; ‘hard’ elements dominate the Cyber Operations Officer recruitment process.

3. Expectations vs. Reality

Our third research question asks, “How do Army Cyber Operations Officers’ actual duties and responsibilities compare with expected/published duties and responsibilities?” This question can be answered directly from the 17A survey, as highlighted in chapter IV, Question 21a, Table 3, which asks respondents if they agree or disagree with the statement, “My current duty position and job responsibilities are in line with my expectations of those of a Cyber Operations Officer (17A) based on the application/recruitment process.” The majority, 53% agree that their actual duties and responsibilities align with expectations, while 18% of respondents say they do not, the remaining respondents did not know or said it was not applicable. Additionally, Question 22 asks respondents, “Are you currently assigned to a position designated for a 17A on your unit’s MTOE?” 55% of the respondents said yes, 36% said no and 9% did not know. Based on our analysis of the data we collected we conclude that the actual duties and responsibilities of Cyber Operations Officers are generally aligned with the expected/published duties and responsibilities.

4. Cyber Leader Aptitude Assessment

Our fourth research question asks, “How do Army methods to measure cyber leader aptitude compare to government and non-military organizations with similar functions?” Army Cyber Branch used the targeted attributes of education, experience, and certifications, in conjunction with the application process, as metrics to determine cyber leader aptitude. A proven tool, the Armed Services Vocational Aptitude Battery-Cyber Test (ASVA-CT), was not used in neither the selection process nor the development of the recruitment pool. The Army Marketing Research Group (AMRG), responsible for research to support accessions, was not consulted or provided any support to the recruitment of Cyber Operations Officers. Psychometric testing used to evaluate a candidate’s ability to solve problems across both logical and physical domains was also not utilized. This led the researchers to the conclusion that the Army did not use all the available aptitude assessment tools at its disposal for both the recruitment and selection processes for Cyber Operations Officers.

5. Implementation Feasibility of other Recruitment Processes

Our fifth and final research question asks, “What elements of nonmilitary HRMs for recruiting cyber leaders are feasible for implementation in an Army HRM for recruiting Cyber Operations Officers?” The Army has several proven models which could be adapted for Cyber Operations Officer recruitment and selection. Both Special Forces and Aviation recruitment models focus on special application of skills that exist in the military and civilian sectors. The aforementioned Army branches use proven aptitude and psychometric testing to provide detailed information about the recruitment pool and selectees. With minor modifications, Special Forces and Aviation recruitment practices could be tailored to provide Cyber Branch with the same level of aptitude assessment.

Because cybersecurity roles and functions are standardized across all of DOD, Army Cyber Branch could use the Cyber Competency Model (CCM) and the Cyber Workforce Framework to inform the Cyber Operations Officer recruiting process. The purpose of the aforementioned documents is to establish a “common language to speak about cyber roles and jobs and helps define personal requirements in cybersecurity.” (NICCS, 2017). The targeted attributes developed by Army Cyber Branch diverge from practices used in other DOD and federal organizations.

Based on the research conducted for this thesis, the Cyber Operations Officer recruitment process would benefit greatly from the addition of an interview process. The lack of an interview process is another indication of the Army’s predisposition for ‘hard’ HRM elements. The data collected from behavioral or situational interviews could improve the effectiveness of the selection process. The regimented nature of Army Officer HRM makes an iterative interview process less feasible due to time constraints.

B. PRACTICAL IMPLICATIONS

First, the MOEs validated through the factor analysis provide another tool to assess candidates in the recruitment pool and to measure process effectiveness post-selection. Pre-selection survey results could refine targeting of officers within the recruiting pool. Post-selection survey data provides valuable feedback to both Cyber Branch and USAREC on the effectiveness of the recruitment process. The data would inform after action reviews which are used to improve or modify how Cyber Operations Officers are recruited.

Second, the evaluation of the Army Cyber Operations Officer recruitment process and comparison with processes in selected organizations offer some insights. First, the Army did not use proven and established tools to assess the aptitude of candidates in the recruitment pool. Our research suggests the ASVAB-CT and psychometric testing provides Cyber Branch a more complete appraisal of an individual’s skills and abilities. These tests provide objective metrics to identify aptitude in candidates who may not meet the education or credential requirements. Also, aptitude testing serves as another method to verify possession of skills stated on the application.

Third, based on current recruitment and selection criteria, our research suggests continuation of the VTIP to ensure the 17A field grade officer population possess the requisite operational and leadership experience. The force structure of 17As does not provide the same opportunities for exposure to tactical and operational activities as the other Army branches. To provide greater assurance that Cyber Operations Officers possess the operational experience, leadership ability, and technical competency, a continual influx of personnel from other occupational specialties appears to be necessary.

Fourth, the standardization of cybersecurity work roles across in the federal government and DOD presents opportunities to incorporate established business practices. Use of the CCM and CWF in the recruitment process keeps the 17A HRM in step with the greater government cybersecurity community. One of the strategic goals of the CWF is recruitment of the cyber workforce. (DOD, 2013). The aforementioned guidelines and standards provide the Army with a template to recruit capable and experienced manpower.

Lastly, the current Cyber Operations Officer recruitment process will eventually force Cyber Branch to make a decision regarding self-sustainment. Offensive and defensive cyber operations are inextricably linked to traditional Army IT functions. Operations and maintenance, information system and network engineering, and most importantly, IT policies, form a complex web of interdependencies with the roles of 17As. Our research suggests that eventually a decision will need to be made to incorporate the aforementioned traditional IT functions into Cyber Branch or to become a special branch like JAGC, the Medical Corps or Special Forces.

C. LIMITATIONS

There were several limitations during the conduct of our research that should be considered when reading our conclusions. First, we were unable to gain access to commonly used objective metrics for measuring the effectiveness of the 17A recruiting strategy. Specifically, performance results and attrition rates from the Army Cyber School and the Cyber Basic Officer Leadership Course (Cyber BOLC) for the 17A population were unavailable. Although less than 20% of survey respondents attended MOS specific training prior to starting in their first 17A position, having access to this metric would have enabled us to develop a more holistic picture of the selected 17As.

Second, we were unable to gain access to Officer Evaluation Reports (OERs) or obtain comparable officer assessments from first line supervisors/raters in our survey. This limited the data we could collect on the performance of the 17A population in their actual duty positions which would have allowed us to assess “customer” and/or “employer” satisfaction. This also highlights the fact that the majority of our results were based on our 17A survey which was analyzed from the perspective of selected 17A officers. However, our research goal was not to generalize results to other Army branches. As such, our findings regarding the 17A recruitment strategy should not be construed to be applicable to other branches.

Finally, there have been additional VTIPs conducted subsequent to the initiation of our study. We did not have access to the results of those VTIPs or any lessons learned which may have been applied in light of any previous VTIPs, therefore they were not considered in our research.

D. RECOMMENDATIONS FOR FURTHER RESEARCH

1. Performance Evaluations as MOEs

We recommend the Army conduct further research on the potential value of using their Officer Evaluation Reports (OERs) and academic efficiency reports (AERs) as measures of effectiveness (MOEs) in the recruitment of Cyber Operations Officers. The OERs of officers selected and not selected could inform the recruitment process. Researchers could identify performance trends in the target population before and after selection. Review of AERs could be used as a predictor for performance in cyber specific training.

2. Impact of Recruitment Process on Demographics

The current Cyber Operations Officer recruitment process created some deviations from overall Army proportions for gender and race. We recommend further research to understand how to maintain diversity in the Army cybersecurity workforce while acquiring personnel with the requisite skills.

3. Training/Development and Retention

As the Army Cyber Branch matures, evaluation of training, development, and retention programs will become necessary to prevent squandering of recruitment efforts. Research on training and development programs could provide necessary feedback on the adequacy and quality of expertise produced by Army schools. More importantly, studies conducted at regular intervals on retention could help the Army maintain a level of competitiveness with other organizations for top cybersecurity talent.

E. CONCLUSION

The Army has spent a large amount of its intellectual capital developing the recruitment and selection process for 17As. Our research builds upon that work to evaluate the effectiveness of that process and identify areas for possible improvement. The cybersecurity workforce provides a unique recruiting challenge for private companies, government agencies, and the military. This study identifies the similarities and differences presented by their respective organizational functions to provide the Army with options to close the competitive gap when recruiting cybersecurity personnel.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. SUPPLEMENTALS

The following appendices are included as supplemental material in order to provide additional context to the research and analysis we conducted. Each appendix is provided to support the creation, distribution and detailed analysis of our Cyber Operation Officers (17A) survey and the data collected from the Person-Event Data Environment (PDE). Additionally, the write-ups and code for the statistical analysis we conducted in partnership with TRAC–Monterey during this research are included in this supplemental.

APPENDIX A—17A SURVEY QUESTIONNAIRE

Appendix A details the specific questions asked in the 17A survey used in this research. It includes each of the question categories (demographic, background/experience, assessment of the recruitment process, job satisfaction, duty description/assignment, performance and motivation). Appendix A can be obtained through the NPS library.

APPENDIX B—17A SURVEY QUESTIONNAIRE RESULTS

Appendix B details the aggregated results of the 17A survey. It includes response rates for all survey questions except questions 38–40, which were open-ended questions. Appendix B can be obtained through the NPS library.

APPENDIX C—TRAC-MONTEREY 17A SURVEY ANALYSIS (FACTOR AND REGRESSION TREE ANALYSIS)

Appendix C is the write up from TRAC–Monterey for the statistical analysis of the 17A survey data, conducted with the assistance of MAJ Jarrod Shingleton. It includes the detailed explanation and coding for the “R” software used to conduct the exploratory factor analysis (EFA) and the regression tree analysis. Appendix C can be obtained through the NPS library.

APPENDIX D—TRAC_MONTEREY 17A SURVEY ANALYSIS (SENTIMENT/TEXT ANALYSIS)

Appendix D is the write up from TRAC–Monterey for the analysis of the 17A survey data open ended questions, conducted with the assistance of MAJ Nathan Parker. It includes the detailed explanation and coding for the "R" software used to conduct sentiment/text analysis. Appendix D can be obtained through the NPS library.

APPENDIX E—PDE DATA: AGE

Appendix E is PDE generated charts that provide the ages and descriptive age statistics for the 17A population. Average age by rank, gender, and both rank and gender are depicted here. Appendix E can be obtained through the NPS library.

APPENDIX F—PDE DATA: GENDER

Appendix F is PDE generated charts that depict the descriptive statistics for gender. Gender proportions for the 17A population are presented by rank, race, and major command, then compared with DOD and Army prop gender proportions. Appendix F can be obtained through the NPS library.

APPENDIX G—PDE DATA: GENDER/RACE

Appendix G is PDE generated charts that depict the gender proportions by race and compare with DOD and Army gender proportions. Appendix G can be obtained through the NPS library.

APPENDIX H—PDE DATA: MAJCOM GENDER

Appendix H is PDE generated pie charts that depict the gender proportions in the five major commands with the most 17As. Appendix H can be obtained through the NPS library.

APPENDIX I—PDE DATA: MAJCOM PROP

Appendix I is PDE generated pie charts that depict the proportion of 17A positions across 24 major commands. Appendix I can be obtained through the NPS library.

APPENDIX J—PDE DATA: EDUCATION

Appendix J is PDE generated charts that depict the number and type of post-graduate degrees earned, by rank, for the 17A population. Appendix J can be obtained through the NPS library.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Armstrong, M. (2006). *A handbook of human resource management practice.* Philadelphia, PA: Kogan Page.

Army Cyber School. (2017, June). Transition panel criteria (officers & warrant officers)—internal review. Presented at Army Cyber School, Ft. Gordon, GA.

Arnold, T., Harrison, R., & Conti, G. (2013). Professionalizing the Army's cyber officer force. *Army Cyber Center*, *1337*(2), 33.

Arthur, J. B., & Boyles, T. (2007). Validating the human resource system structure: A levels based strategic HRM approach. *Human Resource Management Review, 17*(1), 77–92. doi: 10.1016/j.hrmr.2007.02.001

Axelband, E., Paul, C., & Porche III, I. (2014). *The other quiet professionals: Lessons for future cyber forces from the evolution of special forces.* Santa Monica, CA: RAND.

Barber, A. E. (1998). *Recruiting employees: individual and organizational perspectives.* Thousand Oaks, CA: Sage.

Beal, S. (2010). The roles of perseverance, cognitive ability, and physical fitness in U.S. army special forces assessment and selection. U.S. Army Research Institute: Fort Bragg, NC.

Becker, B.E., and Huselid, M.A. (1998). High performance work systems and firm performance: A synthesis of research and managerial implications, *Research on Personnel and Human Resource Management*, 16, pp. 53–101.

Beer, M., Spector, B., Lawrence, P.R., Mills, D.Q., & Walton, R.E. (1984). *Managing human assets*. New York: The Free Press.

Benjamin, B., Keltner, B., Reynolds, K., Robbert, A., & Spranca, M. (1997). *Differentiation in military human resource management*. Santa Monica, CA.: RAND.

Bicksler, B., Conley, R., Elson, S., Engstrom, J., Jenkins, J., Kennedy-Boudali, L., Nemfakos, C., Rostker, B., Temple, D., Williams, W., & Young, S. (2013). *Workforce planning in the intelligence community*. Washington, DC: RAND.

Bigelow, D. (2008). Managing manpower: A fatigued soldier is a sign of poor leadership. *Armed Forces Journal.* Retrieved from http://armedforcesjournal.com /managing-manpower/

Boxall, P.F., Purcell, J., & Wright, P. (2007). The goals of Human Resource Management. Boxall, P.F., Purcell, J., & Wright, P. (Eds.), *The International Journal of Human Resource Management*, 4(3), pp. 645–655. Oxford: Oxford University Press.

Boxall, P.F., Purcell, J., & Wright, P. (2008). Human Resource Management: Scope, Analysis, and Significance. Boxall, P.F., Purcell, J., & Wright, P. (Eds.), *The Oxford Handbook of Human Resource Management.* Oxford: Oxford University Press.

Breaugh, J.A., and Starke, M. (2000). Research on employee recruitment: So many studies, so many remaining questions. *Journal of Management*, 26(3), pp. 405–434.

Brown, J. (2009). Choosing the Right Type of Rotation in PCA and EFA. *JALT Testing & Evaluation SIG Newsletter*, 13 (3) pp. 20 - 25.

Carnegie Mellon University. (2006, Oct.11). Lecture 10: Regression trees. Retrieved from http://www.stat.cmu.edu/~cshalizi/350-2006/lecture-10.pdf

Carter, P., Kidder, K., Schafer, A., & Swick, S. (2017). *The future of the all-volunteer force*. Washington, DC.

Conti, G., Raymond, D., Harrison, R., & Arnold, T. (2015). Shaping the Army’s cyber operation force: the human factor dimension. *Cyber Defense Review.* Retrieved from http://cyberdefensereview.army.mil

Crootof, R., & Hathaway, O. (2012). *The law of cyber attack*. New Haven, CT: Yale Law School.

Cusworth, J.,& Franks, T.R. (2013). *Managing projects in developing countries.* Routledge.

Cyber Center of Excellence. (2014a, August). Cyber Career Field Implementation Plan (CF17 SME Panel & Way Ahead). Presented at CF17 SME Panel, Ft. Gordon, GA.

Cyber Center of Excellence. (2014b, September). Cyber Center of Excellence (Cyber COE). Presented at AFCEA TechNet, Ft. Gordon, GA.

Daugherty, L. & Li, J. (2015). *Training cyber warriors: What can be learned from defense language training*. Santa Monica, CA: RAND.

Daugherty, L., Gazis, J., Harrington, L., Karmarck, K., & Werber, L. (2016). *Officer accession planning: A manual for estimating air force officer degree requirements*. Santa Monica, CA: RAND.

Davis II, J., Johnson, E., O'Connell, C., McCausland, T., Porche III, I., Wilson, B., Wisniewski, B., & Vasseur, M. (2017). *Cyber potential of the army's reserve component*. Santa Monica, CA: RAND.

Department of the Army. (2005). *Armed services military personnel accession testing programs*. (AR 601–222). Washington, DC: Department of the Army.

Department of the Army. (2005). *Selection and training of army aviation officers*. (AR 611–110). Washington, DC: Author.

Department of the Army. (2006). *Officer assignment policies, details, and transfers*. (AR 614–100). Washington, DC: Author.

Department of the Army. (2009). *The army personnel development system*. (AR 600–3). Washington, DC: Author.

Department of the Army. (2014a). *Commissioned officer professional development and career management*. (DA PAM 6003). Washington, DC: Author.

Department of the Army. (2014, Mar. 24.) Human Resources Command stands up Cyber Branch. Retrieved from https://www.army.mil/article/122456/ Human_Resources_Command_stands_up_Cyber_Branch/?from=RSS

Department of the Army. (2014c). *Initial 17A Cyber Branch Voluntary Transfer Incentive Program (VTIP)*. (MILPER Message 14–298). Washington, DC: Author.

Department of the Army. (2014d). *Military human resources management*. (AR 600–8). Washington, DC: Author.

Department of the Army. (2014e). *Recruiting operations*. (USAREC 3–0). Fort Knox, KY.

Department of the Army. (2014f). *Recruiting*. (USAREC 3). Fort Knox, KY.

Department of the Army. (2015a). *How the army runs: A senior leader reference handbook*. Carlisle, PA.

Department of the Army. (2015b). *Personnel and classification testing*. (AR 611–5). Washington, DC: Author.

Department of the Army. (2016, Jul. 15.) Army announces ARCYBER as an ASCC. Retrieved from https://www.army.mil/article/171596/ army_announces_arcyber_as_an_ascc

Department of Defense. (2003). *Department of defense civilian personnel management system* (DoDD 1400.25). Washington, DC: Department of Defense.

Department of Defense. (2005a). *Department of defense policy for civilian personnel* (DoDD 1400.5). Washington, DC: Author.

Department of Defense. (2005b). *Recruiting facilities* (DoDD 5160.58E). Washington, DC: Author.

Department of Defense. (2008). *Undersecretary of defense for personnel and readiness (USD(P&R))* (DoDD 5124.02). Washington, DC.

Department of Defense. (2011). *Accession processing data collection forms* (DoDD 1304.02). Washington, DC: Author.

Department of Defense. (2011). *DOD strategy for operating in cyberspace*. Washington, DC: Author.

Department of Defense. (2013). *DOD cyberspace workforce strategy*. Washington, DC: Author.

Department of Defense. (2015). *The DOD cyber strategy*. Washington, DC: Author.

Department of Defense. (2016, Oct. 24). All Cyber Mission Force Teams Achieve Initial Operating Capability. Retrieved from https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/

Defense Officer Personnel Management Act of December 12, 1980, 94 Stat. 2835.

Dillman, D., Smyth, J., & Christian, L. (2009). *Internet, mail, and mixed-mode surveys: The tailored design method.* Hoboken, NJ: John Wiley & Sons, Inc.

Evans, P., & Lorange, P. (1989). Two logics behind human resource management. Evans, P., Doz, Y., & Laurent A. (Eds.), Human resource management in international firms. London: MacMillan.

Facebook Careers. (2017). Retrieved from https://www.facebook.com/careers/

Fombrun, C.J., Tichy, N.M., & Devanna, M.A. (1984). *Strategic human resource management.* New York, NY: Wiley.

Geetika, P. (2007). Recruitment strategies: exploring the dimensions in the Indian software industry. *Asian Journal of Management Cases* 4(1): 5–25.

Guest, D.E. (1987). Human resource management and industrial relations, *Journal of Management Studies*, 24(5), pp 503–21.

Hallgren, K. (2012). Computing inter-rater reliability for observational data: an overview and tutorial. *Tutorials in Quantitative Methods for Psychology,* 8(1): 23–34.

Hamilton, L. (1992). *Regression with graphics: A second course in applied statistics.* Belmont, CA: Duxbury Press.

Hansen, M. & Nataraj, S. (2011). *Expectations about civilian labor markets and army officer retention*. Santa Monica, CA: RAND.

Harris, R. D., & Morris, J. D. (2016). Cyber talent for unified land operations. *Small Wars Journal*, 12(1). Retrieved from http://smallwarsjournal.com/jrnl/ art/cybertalentforunifiedlandoperations

Herdman, A.O. (2008). *Explaining the relationship between the HR system and firm performance A test of the strategic HRM framework* (PhD Dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. DP19017).

Human Resources Command. (2015, June). Cyber VTIP Round Two Concept. Presented at Human Resources Command (HRC), Fort Knox, KY.

Human Resources Command. (n.d.). Cyber road show. Presented at Human Resources Command (HRC), Fort Knox, KY.

Hogue, H. (2012). Presidential reorganization authority: History, recent initiatives, and options for congress. Congressional Research Service (CRS). Retrieved from https://fas.org/sgp/crs/misc/R42852.pdf

Iles, P., & Salaman, G. (1995). Recruitment, selection and assessment. Storey, J. (Ed.), *Human resource management: a critical text.* London and New York: Routledge.

U.S. Joint Chiefs of Staff. (2011a). Joint Operations. Joint Publication 3–0. Washington, DC: U.S. Joint Chiefs of Staff.

U.S. Joint Chiefs of Staff. (2011b). *Commander's handbook for assessment planning and execution*. Suffolk, VA: U.S. Joint Chiefs of Staff.

U.S. Joint Chiefs of Staff. (2017). *Joint Operations*. Joint Publication 3–0. Washington, DC: Author.

Loughran, D. & Orvis, B. (2011). The effect of the assessment of recruit motivation and strength (ARMS) program on Army accessions and attrition. Santa Monica, CA.

Luo, T., Chen, S., Xu, G., & Zhou, J. (2013). *Trust-based collective view prediction.* New York, NY: Springer.

Legge, K. (1995). Human resource management: a critical analysis. Storey, J. (Ed.), *New Perspectives on Human Resource Management.* Routledge, London: Revivals.

Lewis, C. (1985). *Employee selection*. London: Hutchinson.

Morgan, S. (2015, July 28). Cybersecurity job market to suffer severe workforce shortage. CSO Online. Retrieved from http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

Moustroufas, E., Stamelos I., and Angelis, L. (2015). Competency profiling for software engineers: Literature review and a new model. Karanikolas N.N., Akoumianakis, D., Nikolaidou, M., Vergados, D., & Xenos, M. (Eds.). New York, NY: ACM pp 235–240 DOI= http://dx.doi.org/10.1145/2801948.2801960

National Institute of Standards and Technology. *National initiative for cybersecurity education.* Retrieved from March, 5, 2017, from https://www.nist.gov/itl/applied-cybersecurity/nice

Nisen, M. (2013, June 19). Google HR boss explains why GPA and most interviews are useless. Business Insider. Retrieved from http://www.businessinsider.com/how-google-hires-people-2013-6

Noon, M. (1992). HRM: A map, model or theory? Turnbull, P. B. P., Blyton, P., & Turnbull, P. J. (Eds.), *Reassessing human resource management.* (pp. 16–30). Newbury Park, CA: Sage.

North Atlantic Treaty Organization. (2012). Psychological and physiological selection of military special operations forces personnel. NATO: Brussels, Belgium.

Niehaus, R. J. (1988). Models for Human Resource Decisions. *HR Human Resource Planning*, 11(2), 95.

Officer Personnel Act of 1947, Ch. 512, 61 Stat. 795.

Officer Grade Limitation Act of 1954, ch. 180, 68 Stat. 65.

Office of Personnel Management. (2017, Jan. 31). Classifications & Qualifications. Retrieved from https://www.opm.gov/policy-data-oversight/classification-qualifications/

Office of Personnel Management. (n.d.). Performance management: Performance management cycle. Retrieved September 4, 2017, from https://www.opm.gov/policy-data-oversight/performance-management/performance-management-cycle/planning/developing-performance-standards/

Office of Personnel Management. (1991). *The classifier's handbook*. Washington, DC: Author.

Office of Personnel Management. (2009). *Handbook of occupational groups and families*. Washington, DC: Author.

Office of Personnel Management. (1991). *The classifier’s handbook*. Washington, DC: Author.

Office of Personnel Management. (1991*). Introduction to the position classification standards*. Washington, DC: Author.

Office of Personnel Management. (2007). *Delegated examining operations handbook: A guide for federal agency examining offices*. Washington, DC: Author.

Office of Management and Budget. (2016a). *Cybersecurity strategy and implementation Plan (CSIP) for the federal civilian government*. Washington, DC: Author.

Office of Management and Budget. (2016b). *Federal Cybersecurity Workforce Strategy*. Washington, DC: Author.

Rashmi, T. (2010). *Recruitment management* (1st ed. ed.). Mumbai India: Himalaya Pub. House.

Rodriguez, D., Patel, R., Bright, A., Gregory, D., & Gowing, M. K. (2002). Developing competency models to promote integrated human resource practices, 41(3), pp. 309–324. http://doi.org/10.1002/hrm.10043

Rostker, B., Thie, H., Lacy, J., Kawata, J., & Purnell, S. (1993). *The defense officer personnel Act of 1980: A retrospective assessment*. Washington, DC.

Rostker, B. (2015). *Reforming the american military officer personnel system*. RAND: Arlington, VA.

Rummel, R. (1967). Understanding factor analysis. *Journal of Conflict Resolution,* 11(4), pp. 444–480.

Rynes, S. & Barber, A. (1990). Applicant attraction strategies: an organizational perspective. *Academy of Management Review* 15(2): 286–310.

Saner, L.D., Campbell, S., Bradley, P., Michael, E., Pandza, N., & Bunting, M. (2016). Assessing aptitude and talent for cyber operations. Nicholson, D. (Ed.), *Advances in human factors in cybersecurity: Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity*. (pp. 431–437). Orlando, FL: Springer.

Stone, T. (1989). *Understanding personnel management*. New York, NY: CBS College Publishing.

Storey, J. (1989). From personnel management to human resource management. Storey, J. (Ed.), *New Perspectives on Human Resource Management.* Routledge, London: Revivals.

Storey, J. (1992). *Developments in the management of human resources: an analytical review*. Cambridge, MA: Blackwell Publishers.

Storey, J. (1995). Human resource management: still marching on, or marching out? Storey, J. (Ed.), *Human resource management: a critical text.* London and New York: Routledge.

Sullivan, J. (2013, September 8). A case study of facebook's amazing talent management practices, part 1. Electronic Recruiting Exchange (ERE). Retrieved from https://www.eremedia.com/ere/a-case-study-of-facebooks-simply-amazing-talent-management-practices-part-1-of-2/

Sullivan, J. (2013, September 8). A case study of facebook's amazing talent management practices, part 2. Electronic Recruiting Exchange (ERE). Retrieved from https://www.eremedia.com/ere/a-case-study-of-facebooks-simply-amazing-talent-management-practices-part-2-of-2/

Sullivan, J. (2005, December 5). A case study of google recruiting, part 1. Electronic Recruiting Exchange (ERE). Retrieved from https://www.eremedia.com/ere/a-case-study-of-google-recruiting/

Sullivan, J. (2005, December 5). A case study of google recruiting, part 2. Electronic Recruiting Exchange (ERE). Retrieved from https://www.eremedia.com/ere/a-case-study-of-google-recruiting-part-2/

The R Foundation. (n.d.) What is R? Retrieved September 8, 2017, from https://www.r-project.org/search.html

Tice, J. (2015, June 15). Staffing goals for cyber branch totals nearly 1,300 officers, enlisted soldiers. Army Times. Retrieved from http://www.armytimes.com

Tichy, N., Fombrum, C. & Devanna, M. 1982. Strategic human resource management. Sloan Management Review, 23(2): 47–61.

Townley, B. (1989). Selection and appraisal: reconstituting 'social relations'? Storey, J. (Ed.), *New Perspectives on Human Resource Management.* Routledge, London: Revivals.

Trippe, D. M., Moriarty, K., Russell, T., Beatty, A., & Carretta, T. (2014). Development of a cyber/information technology knowledge test for military enlisted technical training qualification. *Military Psychology*, 26(3), pp 182–198.

Truss, C., Gratton, L., Hope-Hailey, V., Mcgovern, P., & Stiles, P. (1997). Soft and hard models of human resource management: A reappraisal. *Journal of Management Studies*, 34(1). doi:10.1111/1467-6486.00042

U.S. Army Cyber Command. (n.d.a.). Organization History: Establishment of U.S. Army Cyber Command. Retrieved July 18, 2017, from http://arcyber.army.mil/Pages/ARCYBERHistory.aspx

U.S. Army Cyber Command. (n.d.b.). The Work Role Working Group CMF 17 MOSs. Presented at Cyber Work Role Working Group, Ft. Belvoir, VA.

U.S. Strategic Command. (2016, Sep. 30). U.S. Cyber Command (USCYBERCOM). Retrieved from http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/ us-cyber-command-uscybercom/

Wiener, S. (2005). *Military flight aptitude tests*. Thomson and Peterson's: Lawrenceville, NJ.

Yong, A. & Pearce, S. (2013). A beginner's guide to factor analysis: focusing on exploratory factor analysis. *Tutorials in Quantitative Methods for Psychology*, 9(2), p. 79–94.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California