NAVAL
POSTGRADUATE
SCHOOL

MONTEREY, CALIFORNIA

JOINT APPLIED PROJECT REPORT

AN ANALYSIS OF THE U.S. ARMY'S MILITARY OCCUPATIONAL SPECIALTY (MOS) 17C, A COMPARISON OF THE 17C CAREER PATH IN COMPARISON WITH PRIVATE INDUSTRY, AND RETENTION OF 17C SOLDIERS WITHIN THE U.S. ARMY

September 2021

By: Noel C. Osborne Sr.
Derek C. Sanders
Michael Troyanoski

Advisor: Jeffrey R. Dunlap
Co-Advisor: Stephen Mastro (NSWCPD)

THIS PAGE INTENTIONALLY LEFT BLANK

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

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2021	**3. REPORT TYPE AND DATES COVERED** Joint Applied Project Report

4. TITLE AND SUBTITLE AN ANALYSIS OF THE U.S. ARMY’S MILITARY OCCUPATIONAL SPECIALTY (MOS) 17C, A COMPARISON OF THE 17C CAREER PATH IN COMPARISON WITH PRIVATE INDUSTRY, AND RETENTION OF 17C SOLDIERS WITHIN THE U.S. ARMY	**5. FUNDING NUMBERS**
6. AUTHOR(S) Noel C. Osborne Sr., Derek C. Sanders, and Michael Troyanoski	
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.

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

13. ABSTRACT (maximum 200 words)

This thesis surveyed the capabilities, similarities, and differences regarding the Army’s Military Occupational Specialty (MOS) 17C Cyber Operations and the associated difference and similarities between the career paths in the private sector. The question that guided the research was “What are the recruitment, retention, and sustainment issues the U.S. Army is experiencing within the 17C MOS?” Methodology included a comparative analysis of the learning objectives required by the U.S. Army for MOS 17C and private institutions' ability to train personnel to an equivalent knowledge and skill level of a 17C MOS soldier. It was determined that the U.S. Army’s attrition rate is highest between the enlistment periods of thirty-six months through seventy-two months. Reenlistment for the 17C MOS is between thirty and forty percent after a seventy-two-month window. The U.S. Army invests a significant amount of time and funding to train 17C soldiers, and valuable experience is gained over a seventy-two-month enlistment obligation. By offering additional compensation bonuses, similar work-life balance packages, and varying rank enlistment flexibilities, the U.S. Army may be able to sustain its 17C soldiers for the long term.

14. SUBJECT TERMS cybersecurity, Cyber Operations, career paths, Military Occupational Specialty, MOS, 17C	**15. NUMBER OF PAGES** 85
	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

AN ANALYSIS OF THE U.S. ARMY'S MILITARY OCCUPATIONAL SPECIALTY (MOS) 17C, A COMPARISON OF THE 17C CAREER PATH IN COMPARISON WITH PRIVATE INDUSTRY, AND RETENTION OF 17C SOLDIERS WITHIN THE U.S. ARMY

Noel C. Osborne Sr., Civilian, Department of the Army
Derek C. Sanders, Major, United States Marine Corps
Michael Troyanoski, Civilian, Department of the Navy

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN PROGRAM MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2021

Approved by: Jeffrey R. Dunlap
Advisor

Stephen Mastro
Co-Advisor

Raymond D. Jones
Academic Associate, Graduate School of Defense Management

THIS PAGE INTENTIONALLY LEFT BLANK

AN ANALYSIS OF THE U.S. ARMY'S MILITARY OCCUPATIONAL SPECIALTY (MOS) 17C, A COMPARISON OF THE 17C CAREER PATH IN COMPARISON WITH PRIVATE INDUSTRY, AND RETENTION OF 17C SOLDIERS WITHIN THE U.S. ARMY

ABSTRACT

This thesis surveyed the capabilities, similarities, and differences regarding the Army's Military Occupational Specialty (MOS) 17C Cyber Operations and the associated difference and similarities between the career paths in the private sector. The question that guided the research was "What are the recruitment, retention, and sustainment issues the U.S. Army is experiencing within the 17C MOS?" Methodology included a comparative analysis of the learning objectives required by the United States Army for MOS 17C and private institutions' ability to train personnel to an equivalent knowledge and skill level of a 17C MOS soldier. It was determined that the U.S. Army's attrition rate is highest between the enlistment periods of thirty-six months through seventy-two months. Reenlistment for the 17C MOS is between thirty and forty percent after a seventy-two-month window. The U.S. Army invests a significant amount of time and funding to train 17C soldiers, and valuable experience is gained over a seventy-two-month enlistment obligation. By offering additional compensation bonuses, similar work-life balance packages, and varying rank enlistment flexibilities, the U.S. Army may be able to sustain its 17C soldiers for the long term.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

(ISC)^2	International Information Systems Security Certification Consortium
ACI	Army Cyber Institute
AIT	Advanced Individual Training
ANSI	American National Standards Institute
ARCYBER	Army Cyber Command
ARGC	Army Recruiting Guidance Counselor
ASVAB	Armed Service Vocational Aptitude Battery
BT	Basic Training
CCNA	Certified Networking Associate
CEH	Certified Ethical Hacker
CIA	Central Intelligence Agency
CISSP	Certified Information Systems Security Professional
CompTIA	Computing Technology Industry Association
DCO	Defensive Cyberspace Operations
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOD	Department of Defense
FBI	Federal Bureau of Investigation
GT	General Technical
INSCOM	Intelligence and Security Command
IoT	Internet of Things
IP	Intellectual Property
IP	Internet Protocol
IT	Information Technology
MILPER	Military Personnel
MOS	Military Occupational Specialty
MPP	Meritorious Promotion Program
NETCOM	Network Technology Command
NSA	National Security Agency

OCO	Offensive Cyberspace Operations
OCONUS	Outside of the continental United States
ODU	Old Dominion University
PMOS	Primary Military Occupational Specialty
ROI	Return on Investment
ROTC	Reserve Officer Training Corps
SCI	Sensitive Compartmented Information
SGLI	Service Group Life Insurance
ST	Skilled Technical
TS	Top Secret
TAFS	Total Active Federal Service
UN	United Nations
U.S.	United States
USAREC	United States Army Recruiting Command
USCYBERCOM	United States Cyber Command
WBA	Written Bonus Agreement

ACKNOWLEDGMENTS

This thesis was made possible by the hard work and dedication of many individuals across multiple organizations and service branches. The authors would like to thank their advisors, Professor Jeffrey Dunlap, USN (ret.), and Dr. Stephen Mastro for their time, experience, and guidance during the writing and review process as well as the Thesis Processing Office (TPO) and the Graduate Writing Center (GWC) at Naval Postgraduate School (NPS). The authors would also like to extend a thank you to the U.S. Army Recruiting Command (USAREC) for providing valuable data in which our thesis was based on. Lastly, the authors would like to extend a gracious thank you to their families who supported them every step of the way during the late nights and long hours throughout this process.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> Cyber threats pose one of the gravest national security dangers the United States faces. They jeopardize our country's critical infrastructure, endanger our individual liberties, and threaten every American's way of life. When our Nation's intellectual property is stolen, it harms our economy, and when a victim experiences online theft, fraud, or abuse, it puts all of us at risk.
>
> —Barack Obama, 2014

A. IMPORTANCE OF CYBER SECURITY

Cyber security is a relatively new term that has been thrust to the forefront of everyday life in recent years and is defined as "the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks" (Kaspersky, 2021, para. 1). In this light, cyber security touches almost every single individual via direct or indirect methods. Most individuals use a computer or mobile device multiple times throughout the day or a traditional desktop or laptop computer. Servers, electronic systems, and networks are used by many of the same individuals, indirectly, without their knowledge. Electronic data is generated and collected by all devices on a routine basis. Examples of this collected data include an individual's location, healthcare, financial, social preferences, and consumer selections. This collected data is used to sharpen search tools, generate advertising revenue, or even sold for a profit to other entities. With the advent of cloud computing, all electronic devices are connected through what is known as the Internet of Things or IoT (Microsoft, n.d., para. 1). Microsoft defines IoT as "your equipment, machines, products, and devices that are connected to the cloud [internet] and outfitted to collect and securely transmit data" (Microsoft, n.d., para. 1). Cloud computing has made our lives easier providing us access to an unbelievable amount of data and resources at our fingertips. It has improved communication and helped to automate processes and predict outcomes to provide added cost savings and efficiency. Cloud computing has also made it easier for cybercriminals to prey upon the unsuspecting and the unprepared.

All aspects of the modern world are connected to the internet in some way, shape, or form. From infrastructure, banking, and military operations, to childcare, personal vehicles, and even kitchen appliances. The internet is arguably the most important aspect in the daily lives of most Americans whether they know it or not. CompTIA points out that American's specifically are exposed due to the increase of online banking and credit reporting as well as their reliance on supply chains (CompTIA, n.d.b, para. 1). Job payments are made online, bill payments are made online, and mortgages are competed online. Social media allows users to innocently share their accomplishments and tasks then spread them out across the internet. With some easy problem solving and simple data collecting, cyber criminals can gather information via social engineering and do some significant damage such as identity theft (CompTIA, n.d.b, under "Information: What's at Stake"). For those last pieces of information, cyber criminals rely on a tactic known as phishing. Phishing occurs when individuals are targeted with fake advertisements or surveys requiring sensitive information such as bank accounts or social security numbers. Individuals will think they are responding to their banks or a mortgage company when this information is being collected maliciously by bad actors.

Supply chain reliance is also an aspect of life not thought about until it is compromised. Inventory management and ordering are all completed via automated, online processes. Massive amounts of information are flowing from suppliers to producers and back every day which allows suppliers to stay fully stocked and producers to provide enough product to keep the suppliers well stocked. The reliance on the internet connection provides numerous opportunities for cyber criminals to take advantage of lapses in proper cyber security measures.

1. Type of Cyber Crimes

In a 2021 internet posting, Kaspersky, a cyber security firm, classified cybercriminals and threats into three overarching categories which are cybercrimes, cyber-attacks, and cyberterrorism. Cybercrime's goal is to financially gain or cause disruption from malicious activity or data gathering occurring. Examples include consumer data hacks or hacks of companies to gain trade secrets. Figure 1 shows the total reported number of cyber data breaches from 2005 through 2018 by industry sector.

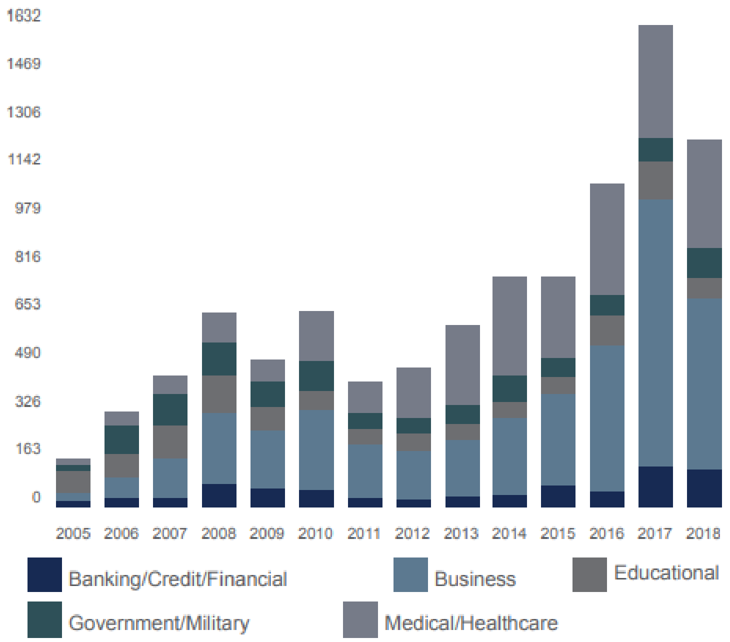


Figure 1. Data Breaches by Industry Sector from 2005 through 2018. Source: Evans and Smith (2019).

Cyber-attacks often are politically motivated and gather data about various targets. Examples here include state actors hacking email accounts of political figures to help opposing candidates gain popularity or conduct smear campaigns against political figures. Cyberterrorism infiltrates electronic systems to cause panic or fear and is defined in more detail by Nick Myers from Old Dominion University (ODU) on a paper written for United Nations (UN) Day 2021. Myers expands on cyberterrorism as the intent is meant to harm, coerce, or intimidate a population or state through cyber activities (Myers, 2021, under “History of Cyber Crime”). Theoretical examples include hacking into traffic networks, water supplies, or power grids to cause widespread chaos or mass casualty situations. (Kaspersky, 2021, under “Types of cyber threats”). These criminals are constantly searching for ways to exploit weaknesses in the general population, but even more concerning are the criminals that seek to do harm to large groups of individuals or entire nations by creating mass hysteria events or crippling aging infrastructure causing daily activities to cease. These attacks often fall into a few basic categories of cyberwarfare like Ransomware Attacks, Distributed Denial of Service (DDoS) and Malware (CompTIA, n.d.b, under "Types of Cybersecurity Threats"). Cybercrime and cyber-attacks are meant to either hold data hostage until a payment or demand is made or met, modifying data, without being detected, or to steal data. Recent examples of ransomware attacks occurred on infrastructure companies such as Colonial Pipeline, Medstar, JBS Meatpacking, as well as a multitude of consumer data breaches such as Target, Marriott Hotels, and Macy's. The federal government is not immune to data breaches either. Frank Konkel (2018) reported via NextGov that the federal government deflects 36 million attempts at hacks per day which equates to over 13 billion attempts per year. In the same article, Konkel also reported that the total data size the DDoS attack attempts were more than 600 gigabytes per second, targeted at unclassified and classified networks owned and operated by the DOD. These hacks and ransomware attacks affect people in a lot of ways. In the most recent cyber-attacks, a mass casualty situation was not the goal of the hackers but may be in the future. This move definitively transfers the issue of cyber threats out of the civilian response world and into the military's scope, who are currently the leading force to combat cyberterrorism and related threats.

2. 17C Military Occupational Specialty (MOS) Need

Military cyber operations are a fast paced, in-demand role tasked with protecting military, Department of Defense (DOD) civilians, contractors, and private industry's intellectual property (IP) and key resources from foreign and domestic cyber threats. The military attracts the best minds and talent and turns them into lethal fighting machines through high velocity training and discipline but has been struggling in recent years to retain these soldiers. In 2010, the United States (U.S.) Senate created a new command within the U.S. Strategic Command and called it U.S. Cyber Command (USCYBERCOM). USCYBERCOM's goals were to provide risk assessments of DOD networks and cyber systems, develop capabilities for computer networks, analyze the operational capabilities of the DOD's cyberspace presence, and conduct cyberspace intelligence operations. Conducting business in these four areas, USCYBERCOM was intended to effectively integrate cyberspace operations across the DOD enterprise which results in a strategic deterrence to future attacks (Lopez, 2010, pp, 16–20).

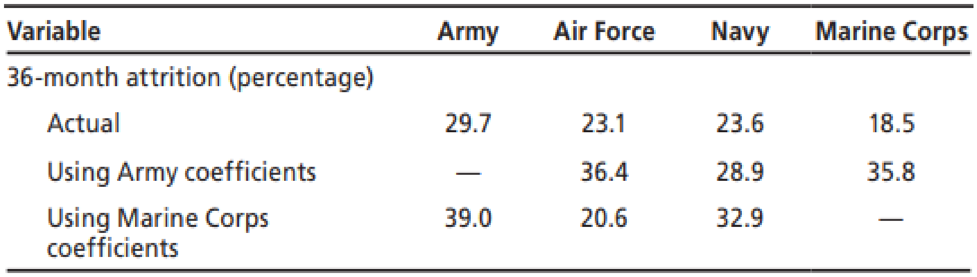
"In 2014, the Army recognized the cyber career field as a basic branch, which includes the 17C Military Occupational Specialty (MOS) for enlisted Cyber Operations Specialists," (Wenger et al., 2017, pp. 1). By training and retaining the best cyber security professionals, the United States Army's 17C MOS category will be able to defend the nation against even the most complex cyber threats and provide a swift response. During a brief in 2018 covered by DOD news reporter Jim Garamone, Daniel Coats, then-director of National Intelligence (DNI), stressed the continued threat of state and non-state actors attempting to cause harm to the U.S. through a multitude of cyber-attacks. This reinforces the need for the Army to reevaluate and strengthen its recruiting and sustainment efforts in the 17C MOS. Coats stated that "from U.S. businesses, to the federal government, to state and local governments, the United States is threatened by cyberattacks every day. Some of these actors, including Russia, are likely to pursue even more aggressive cyberattacks with the intent of degrading our democratic values and weakening our alliances," the intelligence chief said. "Persistent and disruptive cyber operations will continue against the United States and our European allies, using elections as opportunities to undermine democracy, sow discord and undermine our values," (Garamone, 2018, under "Competition for Technological Superiority").

3. Retention and Attrition Issues

"Army leadership is concerned that the Army will have difficulty retaining cyber talent because personnel will be lured by lucrative cyber jobs in the civilian labor market," (Wenger et al., 2017, pp. 3). The workload is high, stress levels are high, and salaries are low when compared to their civilian counterpart positions. A study conducted in 2009 by the Partnership for Public Service and Booz Allen Hamilton uncovered four main issues causing retention and sustainment issues for the Federal Cybersecurity Workforce. Issues stemmed from the following areas: a small talent pool for new hires, the inability to meet federal cybersecurity workforce needs due to fragmented coordination and uncoordinated leadership, complex processes and procedures addressing recruitment and retention, and a disconnect between human resources and front-line managers (Lopez, 2010, pp, 16–20). Armed with new training and certifications that will follow them, the 17C MOS soldiers exit the Army after fulfilling their commitments and seek private corporations with higher pay, flexible hours, and lower stress levels. These fresh, ex-17C soldiers are highly marketable and qualified candidates when the information technology (IT) certifications are combined with security clearances. Now civilians, this enables them to move forward in their careers leaps and bounds when compared to their old positions. The attrition rate is high when compared to the other specialties. The 2017 RAND Corporation study conducted by Jennie Wenger and others concluded that the overall U.S. Army attrition rate was around 25 percent while the 17C MOS hovered around 6 points less which equates to a 19 percent attrition rate (Wenger et al., 2017, pp. 17).

A 2020 RAND Corporation study conducted by James Marrone found that the U.S. Army has the highest attrition numbers when compared to the other services shown in Table 1.

Table 1. Actual Attrition Rates for Military Services from FY 2001 through FY 2013 for the First 36 Months. Source: Marrone (2020).



Variable	Army	Air Force	Navy	Marine Corps
36-month attrition (percentage)				
Actual	29.7	23.1	23.6	18.5
Using Army coefficients	—	36.4	28.9	35.8
Using Marine Corps coefficients	39.0	20.6	32.9	—

Note: Actual rates are based on recruiting data where calculated rates were shown to compare attrition rates between services and how candidates were better off suited in specific service branches. Marrone included FY2013 which carries the 36-month period through 2017.

From an Army career field deficit perspective in addition to high attrition rates, sustainability is growing issue faced by the MOS as well as a financial issue. Each 17C recruit costs the Army $70,000 in training tuition (Wenger et al., 2017, pp. 6). As the Army continues to only sustain its cyber forces, private industry continues to lure candidates away with better careers and additional advancement opportunities. With no forward progress and advancement by private industry the Army is slowing receding in their cyber abilities. In other words, stagnation without progression becomes regression. It is important that the Army address these attrition issues with the 17C MOS position and make fundamental changes to allow 17C MOS soldiers to seek long term careers within the Army that provide competition to private industry equivalents. This will help to reinforce the Army's strength in cyber security and help to build a knowledge base and instill confidence in the solider who chose to make a long-term career with the Army. Without the knowledge base and experience or a plan to address retention, the Army, and the greater DOD will start to lack the necessary skills and specialized personnel to fight and defend state sponsored threats that the United States is facing and will continue to face throughout the age of information.

B. SCOPE OF RESEARCH

This thesis identifies data that correlates with the 17C MOS to establish reasoning why the Army is encountering the challenges with retention and sustainment of trained personnel such as the Cyber Specialists in the 17C MOS. It also highlights and analyzes the problems and concerns connected to the Army's ability to retaining Cyber Soldiers under the 17C MOS. Other secondary factors that are analyzed include the following:

- Civilian cyber security occupations that include the trainings that are similar or equal to the 17C MOS training requirements

- Information Technology (IT) in corporate America encompasses similar cyber security training like that offered by the 17C training program. What is the overlap or gap that exists with regards to the 17C MOS training and certification program when compared to private industry?

- Salaries and benefits that 17C MOS soldiers would find in private industry that are not being offered to them by the Army. Are private corporations offering above and beyond the compensation packages offered by the United States Army 17C MOS? Are they also offering additional training and certification programs not available to 17C MOS soldiers while enlisted?

- This thesis determines how employment opportunities in the civilian IT community are impacting the retention and sustainment of 17C MOS soldiers in the Army. It culminates with recommendations, based on conclusions drawn from findings in literature, on potential programs, policies, processes, procedures, and systems for how the Army can identify, recruit, train and retain the 17C MOS workforce and move towards sustainment of the program after retention has been addressed.

C. METHODS OF CONDUCTING RESEARCH

Research for this thesis was conducted through a series of literature surveys and working knowledge of the United States Army Recruiting Command (USAREC) processes through personal experience and requested data from USAREC. The data for the 17C position was sourced from USAREC to measure how many individuals that take the Armed Service Vocational Aptitude Battery (ASVAB) to determine the number of applicants that achieve a qualifying score for the Occupational Specialty of 17C. The assessment measures the 17C Occupational Specialty amid other potential enlistees to assess the potential for incentivize applicants that qualify and meet the standard set forth by the Army for the Occupational Specialist to enlist as Cyber Specialists. In addition to the literature survey and personal knowledge of the thesis authors from prior experience, an analytical data driven review is presented to examine the likeliness of 17C's to remain enlisted and continue through their first term of enlistment then reenlist for a second term in the Army. A comparative analysis is offered to define the following topics

- What is the specific training received by 17Cs that causes Industry's desire to recruit them?

- What would the training cost in corporate? What are the wage differences between a trained Cyber Operations Specialist and his/her civilian counterpart?

- What is the overlap between 17C and the civilian occupation, (i.e., Information Security) that propels the attraction for Army Veterans?
- What is the median/average/intermediate income of a 17C versus his civilian counterpart with equal training, (i.e., certification(s))?

D. THESIS ORGANIZATION

1. Introduction

The first chapter, Introduction, outlines the importance of the thesis, research scope, methods of research collection, and organization of the thesis. This chapter provides a brief background on cybersecurity in both the civilian and military worlds as well as highlights current retention issues the Army is experiencing and define a few major cyber-attacks in recent years. This helps to define the issue the nation is facing and underline the importance of training and retaining cybersecurity specialists, specifically Army 17C recruits, to combat the ever-growing threat.

2. Background

The second chapter, Background, outlines the history of the 17C MOS in the Army and provides a foundation for why 17C was created and how it came to be the position it is today. This chapter aims to develop the 17C MOS in full detail to allow the reader to understand how the positions functions and its importance to the Army. Included in this chapter are the Army's 17C qualifications for Cyber Security MOS. These are compared to the civilian equivalent to show how they relate. The 17C MOS position is a critical position and therefor requires a specific set of skills to qualify for it. These qualifications are defined here along with the employment criteria for those enlisted under this MOS. Post enlistment brings a multitude of training programs that recruits must undergo to grow their toolkit and be developed into a capable cyber soldier. These trainings are equivalent to civilian trainings in this field have fully burdened costs tied to them. This helps to develop a picture of what the Army spends on each 17C soldier and why retaining them is a critical task.

3. Data

The third chapter, Data, presents data collected from the literature surveys and USAREC requests. It builds a case for the retention issue that the Army is facing through facts from multiple sources. The authors compare this to matching jobs and employment opportunities in the civilian sector. This creates the case that recruits do in fact have arguably more lucrative, options outside of the Army when armed with the skills and training collected from their time in the 17C position. Data is presented for pay scales, benefits, and further career advancements between a military career versus a civilian career using the civilian equivalent of a 17C MOS which is an Information Security Analyst I. Retention data from past years will be presented to show the loss of 17C recruits only after a few years.

4. Analysis

The fourth chapter, Analysis, presents the data shown in Chapter III but provides rationale for why the data shows the trends it does. This section describes and analyzes the main reasons why the Army has retention issues and why recruits choose to leave for private sector careers based on the data presented in Chapter III. It also defines any trends that were uncovered during research as well as any inconsistencies that require further investigation. Interpretation of the data presented in Chapter III is provided to conclude Chapter IV.

5. Conclusions and Recommendations

The fifth and final chapter, Conclusions and Recommendations, provides input, based on the data and analysis in Chapter III and Chapter IV, on how the Army can address the retention issues found in the 17C MOS rank based on conclusions drawn. Comparisons are reiterated between the Army and private industry. Suggestions are provided to create new programs or subsidies to entice recruits to remain in the position for longer time periods. Any data found to require more analysis or research is noted for further investigation in the future and specific topics are addressed.

II. BACKGROUND

A. HISTORY OF CYBER COMMANDS IN THE U.S. ARMY

In the 1980s and 1990s, when information technology was in its infancy, individual units of the Army were responsible for planning and implementing their own cyber security based on their specific, operational requirements. As more and more systems became reliant on the internet, the Army realized that protection against vulnerabilities had to be addressed. The Network Technology Command (NETCOM) was established to invest the authority to manage and defend the Army's enterprise-level data networks, known as LandWarNet, under a single authority (U.S. Army, n.d.a. under "Early 2000: Increasing Need for Network Security").

As data systems continued to become more ingrained to the Army's successful operations, 2004 saw the merger of NETCOM with the Intelligence and Security Command's (INSCOM) computer emergency response team. This team, headquartered at Ft. Belvoir, VA, was tasked with the security of Army's information technology systems throughout the force (U.S. Army, n.d.a. under "2004: Theater Operations"), ultimately leading to the creation of the 1st Information Operations Command.

In June of 2009, Secretary of Defense Robert Gates established a new command within the military to oversee all cyber operations. Secretary Gates commented that this move by the Pentagon "will reshape the military's efforts to protect networks from attacks by hackers, especially those from China and Russia. It also consolidates the largest concentration of cyber warriors and investigators in the government under one military command" (Gorman, 2009, para. 3). On October 1, 2010, U.S. Army Cyber Command (ARCYBER) was established at Fort Belvoir under the direction of Army Chief of Staff George W. Casey. ARCYBER created, trained, and deployed specialized teams, known as Cyber Mission Force teams across the force to focus trained cyber operators to support operational requirements (U.S. Army, 2010, para. 2).

In 2013, Army Chief of Staff General Odierno approved and developed the Cyber School at Ft. Gordon to formally establish and train professional Cyber Operators to serve in all levels of the Army. The Cyber School's mission "is to provide the Army with a highly skilled, agile, and innovative Cyber workforce, trained to Army and Joint standards, to fulfill commanders' strategic, operational, and tactical requirements within the Cyberspace domain" (U.S. Army Cyber School, 2020a, para. 1). This school developed the Army career fields of Cyber Operations Officer (17A), Cyber Operations Technician (170A), and Cyber Operations Specialist (17C) and officially adopted them on 1 October 2015.

B. BASIC AND ADVANCED INFORMATION TECHNOLOGY (IT) SKILLSETS AND QUALIFICATIONS

The Computing Technology Industry Association (CompTIA) is a professional organization that provides training, advocacy, resources, and research for IT professionals throughout the world (CompTIA, n.d.a, under "Who is CompTIA"). Their certifications are the standard for IT professions in private industry as well as the 17C soldiers. Other industry standard certifications are the Certified Ethical Hacker (CEH), an American National Standards Institute (ANSI) accredited certification, provided by multiple vendors, Certified Information Systems Security Professional (CISSP) license which was created by the International Information Systems Security Certification Consortium $(ISC)^2$, and the CISCO Certified Networking Associate (CCNA) created by Cisco.

1. CompTIA A+ Certification

One of the most common CompTIA certification programs available is the A+ certification. Under the A+ program, candidates should understand the basic operations and maintenance of traditional IT components such as mobile devices, personal computers or desktops, and laptops. There are two exams required to earn this certification which are designated Core 1 and Core 2. Core 1 covered basic IT skills for entry level professional and Core 2 covers more software-based installation, security and troubleshooting processes. Some of the topics covered include in the preparation program include (Study.com, 2021, under "A+ Certification Program"):

- Computer components
- Installation

- Maintenance
- Upgrading computer systems

2. CompTIA Network+ (Net+) Certification

The CompTIA Net+ programs that prepares students for the CompTIA Net+ certification is commonly found at a variety of community colleges and technical schools. The Net+ certification requires individuals to pass a 90-minute, multiple-choice exam (Study.com, 2021, under "Network+ Certification Programs"). Competency domains that the Net+ exam and certification cover topics in the following knowledge areas:

- Network theory
- Network components
- Network operating systems
- TCP/IP networks
- Local area and wide area networks
- Wireless networking

3. CompTIA Security+ (Sec+) Certification

CompTIA Security+ certification focuses on competency domains which include skills to identify attacks or malicious code, implement access controls, identify, and repair common security issues, policy and procedure creation and maintenance, application development, and basic cryptography operations. Functional career fields that support certifications in Sec+ are outlined by the organization ONLC Training Center in their learning material for course preparation:

- Security architect
- Security engineer
- Security consultant/specialist
- Information assurance technician
- Security administrator

- Systems administrator and network administrator (ONLC Training Centers, n.d., under "Overview").

4. Certified Ethical Hacker (CEH):

The Certified Ethical Hacker (CEH) certification is offered by the International Council of Electronic Commerce Consultants (EC-Council). The certification is a well-known and established security certification centered around offensive cyber operations. Paul Jackson wrote an article for the IT training community website, Quickstart, and described some highlights of the benefits for attaining the CEH certification. The CEH certification is ANSI-accredited, and DOD Directive 8140-approved which allows security professionals working in both the public and private sectors to benefit from it. Jackson outlines some key attributes when planning for the CEH certification which are

- CEH with Training: Average $4,000
- The base costs for CEH with EC-Council-approved training:
- CEH training: $850 to $2,999
- CEH exam fee: $1,199
- CEH remote proctoring: $100
- The total cost of the CEH: $2,149 to $4,298 (Jackson, 2020, para. 1).

5. Certified Information Systems Security Professional (CISSP):

The CISSP certification is one of the more intensive certifications in a cybersecurity professionals toolkit. The organization Cybersecurity Education outlines ten major topic areas that the CISSP focuses on which are "access control systems and methodology, business continuity planning and disaster recovery planning, physical security, operations, security, management practices, telecommunications, and networking security," (Cybersecurity Education, n.d., under "What is the CISSP?"). Some key attributes of the CISSP certification are (Iqbal, 2021, para. 2):

- Course fee: $300 to $3,200

- Exam fee: $699

- Preparation time: 50 to 70 hours (cost depends on hourly rate)

6. CISCO Certified Networking Associate (CCNA):

- The CISCO Certified Networking Associate (CCNA) certification encompasses functional areas of networks and network theory essentials defined by CISCO as basic network access, Internet Protocol (IP) connectivity, IP services, security fundamentals, and automation programmability (CISCO, n.d., under "One training course, one exam"). Some key attributes of the CCNA certification include (ASM Educational Center, n.d., under "Overview")
- Boot Camp: 5 Days
- Evening Courses which are held 2 nights per week
- Virtual/WebEx certification availabilities
- Price (All Inclusive): $3,295.00

C. 17C QUALIFICATION CRITERIA

1. Requirements for the Army Cyber Institute (ACI)

Prior to enlistment into the United States Army, a potential MOS 17C candidate should enroll for the Armed Service Vocational Aptitude Battery (ASVAB). This examination measures each applicant's trainability. The ASVAB provides a benchmark to inform the Army of which MOS a trainee would be most successful in. This enables the Army to select the best fit MOS the first time thus minimizing wasted training dollars on candidates who may switch MOSs. "To become one of the cyber operations specialists, you must have a 110 on your GT (General Technical) where you will be exposed to word knowledge questions, paragraph comprehension, and arithmetic reasoning. Also, you must obtain a 112 on your ST (Skilled Technical) focusing, again, on your word knowledge, paragraph comprehension, general science, mechanical comprehension, and mathematics knowledge," (Job Test Prep, 2021, under "Requirements for Cyber Institute"). Table 2 summarized the ASVAB lines scores required for 17C MOS eligibility.

Table 2. ASVAB Line Scores Required for Enlistment in 17C MOS. Adapted from Piha (2021).

MOS	Title	Skilled Technical (ST) Line Score	General Technical (GT) Line Score
17C	Cyber Ops Specialist	≥ 112	≥ 110

2. Minimum Requirements for 17C Qualification Criteria without ASVAB Test Scores

This list of minimum requirements for entry into the 17C MOS is defined by the U.S. Army Cyber School. These minimum requirements are in addition to the ASVAB test scores outlined in Table 2:

- A physical demands rating of medium.
- A physical profile serial system rating of 222221 (Smith, 2019, under "Physical Profile Serial System").
- Normal color vision.
- A high school graduate or equivalent prior to entry on active duty.
- Never been a member of the U.S. Peace Corps, except as specified in AR 614-200 (para 3–2).
- No information in military personnel, Provost Marshal, intelligence, or medical records that would prevent the granting of a security eligibility under AR 380-67 (para 2–4).
- No record of conviction by court-martial.
- No record of conviction by a civil court for any offense other than minor traffic violations.
- Must be a U.S. citizen.
- The Soldier must have a SECRET clearance to apply but they must meet interim TOP SECRET (TS) Sensitive Compartmented Information (SCI) access eligibility requirements prior to course attendance and to be awarded MOS, then final adjudication to maintain MOS.
- No waivers for any of the requirements (U.S. Army Cyber School, 2020b, under "Minimum Requirements").

D. THE ARMY CYBER INSTITUTE ADVANCED INDIVIDUAL TRAINING (AIT) CERTIFICATIONS VERSUS INDUSTRY EQUIVALENT CERTIFICATIONS

The training plan required for individuals accepted into the Army's Cyber Security Program, outlined by Elie Piha on the website Operation Military Kids which provides information on military career paths, consists of a demanding 13 months which is divided into the following two courses and durations:

1. The introductory training is 25 weeks (about 5 and a half months) and commences in Pensacola Florida at the Naval Air Station.
2. The subsequent 20 weeks (about 4 and a half months) of training is conducted at Fort Gordon Georgia at the Headquarters to the United States Army Cyber School (Piha, 2021, under "How long is AIT for cyber security").

At the conclusion of the training courses for the 17C MOS career field, candidates will have certifications for: CompTIA A+, CompTIA Network+, CompTIA Security+, Certified Ethical Hacker (CEH), Certified Information Systems Security Professional CISSP), CISCO Certified Networking Associate (CCNA), which are defined in Table 3.

Individuals that complete the Army Cyber Security Training can expect to be stationed in three stateside locations: Fort Gordon, GA; Fort Lackland, TX; and Fort Meade, MD. Outside of the continental United States (OCONUS), Schofield, HI.

To receive similar certifications through industry, the requirements are twofold: register for boot-camp training in each of the respective certificate element or enrollment in a college or university to earn a degree in Cyber Security and then take the certifications separately. In either case, individuals are addressing a requirement of a minimum of 4 months, (i.e., boot-camp only) or 4 years and 4 months with the college degree approach then taking the boot-camps to obtain the certification (Piha, 2021, under "Training").

Table 3. 17C Training Comparison between Military Cyber Operations Specialist and Industry

Training Obtained through Army Training	17 C Training	Industry
CompTIA A+	Free with Army Training	5 Days $2,495.00 Boot-Camp, ~$500.00 per day
CompTIA Network+	Free with Army Training	5 Days $2,495.00 Boot-Camp, ~$500.00 per day
CompTIA Security+	Free with Army Training	5 Days $2,495.00 Boot-Camp, ~$500.00 per day
Certified Ethical Hacker (CEH)	Free with Army Training	5 Days $4,000.00 Remote fee, Training, Proctor & Exam, Boot-Camp, ~$800.00 per day
Certified Information Systems Security Professional (CISSP)	Free with Army Training	5 Days $2,195.00 Boot-Camp, ~$439.00 per day earns ~$113,000.00 per year
CISCO Certified Networking Associate (CCNA)	Free with Army Training	20 Weeks $6,000.00 Boot-Camp, ~$439.00 per day

There is no authoritative database that states what the cost for the training would be through industry. Notwithstanding, the data provided in Table 3 is an average of the costs incurred through various sources. A candidate looking for these certifications can find them offered through several various sources all of which may have slightly difference costs.

Comparatively, a soldier who graduates from the 17C MOS program, with all related certifications, is far more valuable to the commercial, industrial information technology, and cyber security fields than a civilian that completes a similar certification tract. The soldier has real-life, hands-on performance-oriented training, practical experience identifying and overcoming cyber security vulnerabilities and attacks and be able to provide value to the organization immediately upon starting employment. The civilian with the same certifications has completed several practical training exercises based on fictional scenarios and may or may not be as effective on their first day on the job. The experience that comes with the soldier's cybersecurity training tract is invaluable where the basic training and lab work that the civilian has completed can only be leveraged when a real-world cybersecurity incident is presented.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DATA

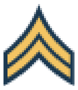
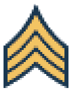
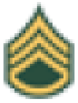
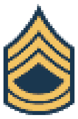
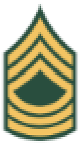
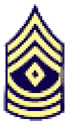
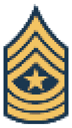
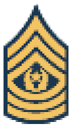
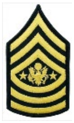
Chapter III, Data, presents relevant data and descriptions for the military service and civilian sectors pertaining to various forms of compensation. This is done to show a direct comparison between the 17C MOS and the civilian equivalent. After compensation data is presented, data related to retention and sustainment efforts is presented. This data is included to demonstrate to the reader that there is an issue with 17C soldiers and the continuation of service. Lastly, methods of incentivizing soldiers to extend service is presented to show that the U.S. Army understands the issue and is working towards a solution.

A. PAY VARIATION BY RANK

Despite the refined and difficult nature of the Cyber Operations Specialists work within the U.S. Army, the pay remains the same as it relates to all Military Occupational Specialties (MOS). "…the pay for Army Cyber Operations Specialists is dictated based on Army rank and years of service," (Piha, 2021, under "What does an Army Cyber Operations Specialist make?"). Table 4 outlines the enlisted rank and associated minimum monthly pay

Table 4. Monthly Pay by Rank. Adapted from Piha (2021)

Insignia	Pay Grade	Rank	Abbreviation	Minimum Monthly Pay
	E-1	Private	PVT	$1,785
	E-2	Private Second Class	PV2	$2,001
	E-3	Private First Class	PFC	$2,104
	E-4	Specialist	SPC	$2,330

Insignia	Pay Grade	Rank	Abbreviation	Minimum Monthly Pay
	E-4	Corporal	CPL	$2,330
	E-5	Sergeant	SGT	$2,542
	E-6	Staff Sergeant	SSG	$2,775
	E-7	Sergeant First Class	SFC	$3,208
	E-8	Master Sergeant	MSG	$4,480
	E-8	First Sergeant	1SG	$4,480
	E-9	Sergeant Major	SGM	$5,473
	E-9	Command Sergeant Major	CSM	$5,473
	E-9	Sergeant Major of the Army	SMA	$5,473

Note: During training, candidates are still compensated monthly through biweekly installments.

B. BASIC PAY CHART FOR ACTIVE-DUTY SOLDIERS*

The pay scale in Table 5 "reflects Basic Pay only and does not include bonuses, allowances and other benefits," (U.S. Army, 2019, under "Basic Pay Chart for Active-Duty Soldiers") From Private E1 – Specialist/Corporal E4.

Table 5. Annual Pay by Rank for Enlisted.* Adapted from U.S. Army (2019).

Rank	<2 Years' Experience	4 Years' Experience	6 Years' Experience	8 Years' Experience
Private (E1)	$21,420.00**	$21,420.00	$21,420.00	$21,420.00
Private (E2)	$24,008.40	$24,008.40	$24,008.40	$24,008.40
Private First Class(E3)	$25,246.80	$28,461.60	$28,461.60	$28,461.60
Specialist or Corporal (E4)	$27,964.80	$32,562.00	$33,948.00	$33,948.00

*Based on 2021 pay tables.

**Pay for Private (E1) will be slightly lower for the first four months of service.

C. TOTAL ARMY COMPENSATION

To understand how civilian wages, compare to those of their service member counterparts, a holistic view must be taken to identify all forms of military compensation. Benefits earned by members of the United States Armed Forces fall into one of two broad categories, base pay, and common allowances. The sum of base pay and common allowances make up a soldier's total compensation.

1. Base Pay

Service members earn pay monthly, paid in bi-weekly increments. This pay varies from service member to service member based on rank and time in service, but totals are consistent across all branches of the Armed Forces. This means, for example, an E-2 in the Army with over two years of service will make the same amount of base pay as a Marine E-2 with over two years of service. Table 6 outlines the base pay amounts for the first-term soldiers as of 2021 with varying time of service categories included.

Table 6. Monthly Base Pay with Time of Service. Adapted from Military Benefits (2021).

Pay Grade	2 Years of Less	Over 2 Years	Over 3 Years	Over 4 Years	Over 6 Years
E-1	$1,785	$1,785	$1,785	$1,785	$1,785
E-2	$2,001	$2,001	$2,001	$2,001	$2,001
E-3	$2,104	$2,236	$2,372	$2,372	$2,372
E-4	$2,330	$2,450	$2,582	$2,714	$2,829
E-5	$2,542	$2,713	$2,844	$2,978	$3,187

2. Common Allowances

Allowances are additional funds that allow the service member to conduct their Military Occupational Specialty efficiently. The amount of compensation a service member receives changes from member to member and is reliant on multiple factors such as geographic location, rank, type of duty, marital status, and number of dependents. Common types of allowances include:

a. Basic Allowance for Housing

These are funds given to a member so that they can provide housing for themselves and their dependents (Pay and Allowances of the Uniformed Services, 2013). The amount is based geographic location, rank, marital status, and number of dependents.

b. Basic Allowance for Subsistence

These are funds provided to offset the costs associated with a service member's meals. The amount is based on rank.

c. Overseas Housing Allowance

These are funds provided to service members overseas to pay for housing. The amount is based on geographic location, marital status, number of dependents, and rank.

d. Clothing Allowance

These are funds provided to enlisted service member to assist in the purchasing and upkeep of uniform items

The combination of a service member's base pay, and the sum of their individual allowances make up their total compensation. It is important to note that base pay is not MOS specific. An E-2 17C Cyber Operator earns the same pay as an E-2 11B which is Army Infantrymen, a non cyber role. Since the common allowances amount varies from service member to service member, this thesis will focus on the base pay of soldiers when compared to the base salary of their civilian counterparts. The following section will highlight civilian wages in the cyber community within a similar role to the 17C soldier.

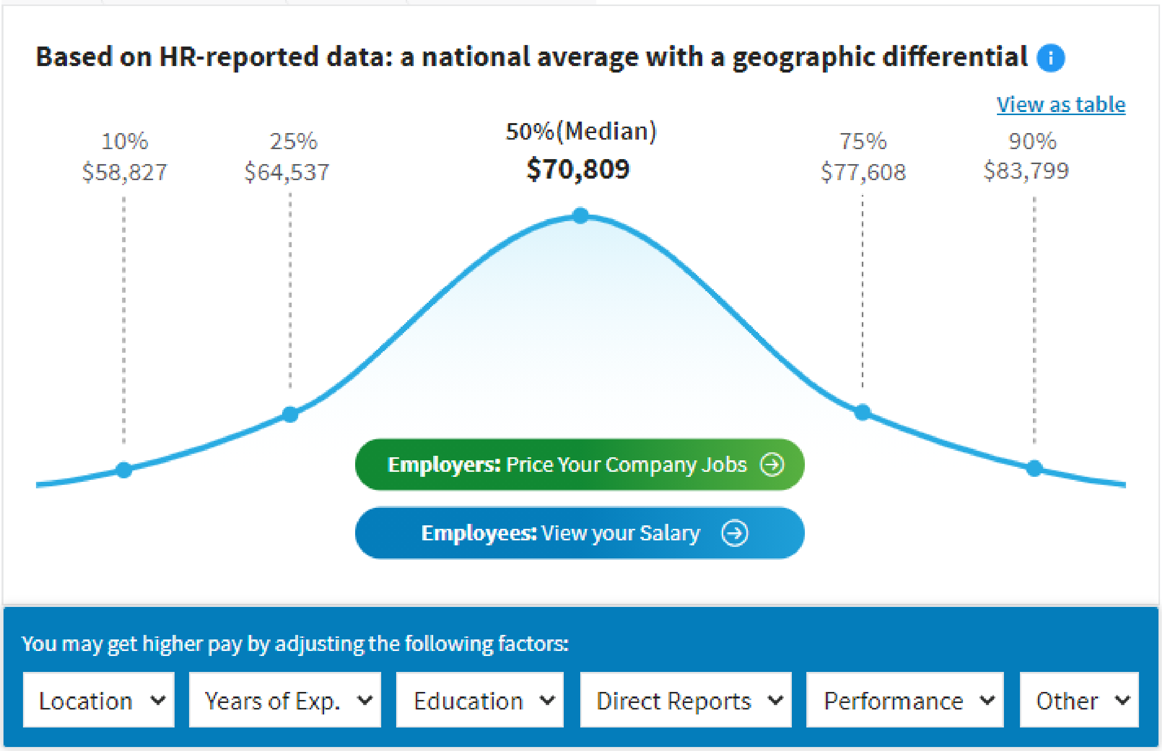
D. CLEARANCES

An ex-17C soldier has quite the gamut of certifications and qualifications, as shown in Table 3, but he also holds another valuable qualification, which is his security clearance. The cost associated with obtaining a SECRET clearance can be as much as $3,000, but the cost of a TOP SECRET clearance runs between $3,000 and $15,000 (TAOnline, 2021, para. 1). This disparity in prices occurs due to geographic location and the amount of time/work required to complete the clearance process. By hiring former soldiers that have obtained a clearance at the expense of the government, private organizations achieve an immediate Return on Investment since they are not required to pay for the employee's clearance. Not only are private organizations saving on the clearance process but individuals who hold clearances have been properly vetted and are mostly trustworthy, reliable individuals who will provide value to a team.

Another benefit for the company hiring former soldiers is their ability to save time in the clearance process. "Current Top Secret clearance processing times are 159 days, and Secret clearance processing times are 132 days" (Kyzer, 2021, para. 1). When a position requires a TS SCI clearance, a former solder can provide 159 days of productivity while someone lacking a clearance is navigating through the clearance process. This immediate return on investment (ROI) is an extreme benefit to companies looking to hire new employees to fill TS SCI designated billets.

E. CIVILIAN WAGES – INFORMATION SECURITY ANALYST I

The civilian equivalent of an Army soldier under the 17C MOS – Cyber Operations Specialist is known as an Information Security Analyst or Cyber Security Analyst I. These two civilian sector positions closely match what entry level 17C soldiers would consider job responsibilities. Information Security Analysts "plan and carry out security measures to protect an organization's computer networks and systems" (U.S. Department of Labor, 2021, under "What Security Analysts Do"). An Entry Level Cyber Security Analyst "completes tasks designed to ensure the security of the organization's systems and information assets," (Salary.com, 2021, under "Job Description"). The salary for an Entry Level Cyber Security Analyst in the United States of America falls in the range of $64,537 and $77,608, with a median of $70,809 (Salary.com, 2021, para.1), as shown in Figure 2.



Based on HR-reported data: a national average with a geographic differential

You may get higher pay by adjusting the following factors:

Figure 2. The Salary for an Entry Level Cyber Security Analyst in the United States of America. Source: Salary.com (2021).

The *U.S. Department of Labor Occupational Outlook Handbook* also provides data on Information Security Analysts and advertises the median annual wage as $103,590.00 (U.S. Department of Labor, 2021, under “What Security Analysts Do”), as shown in Figure 3.

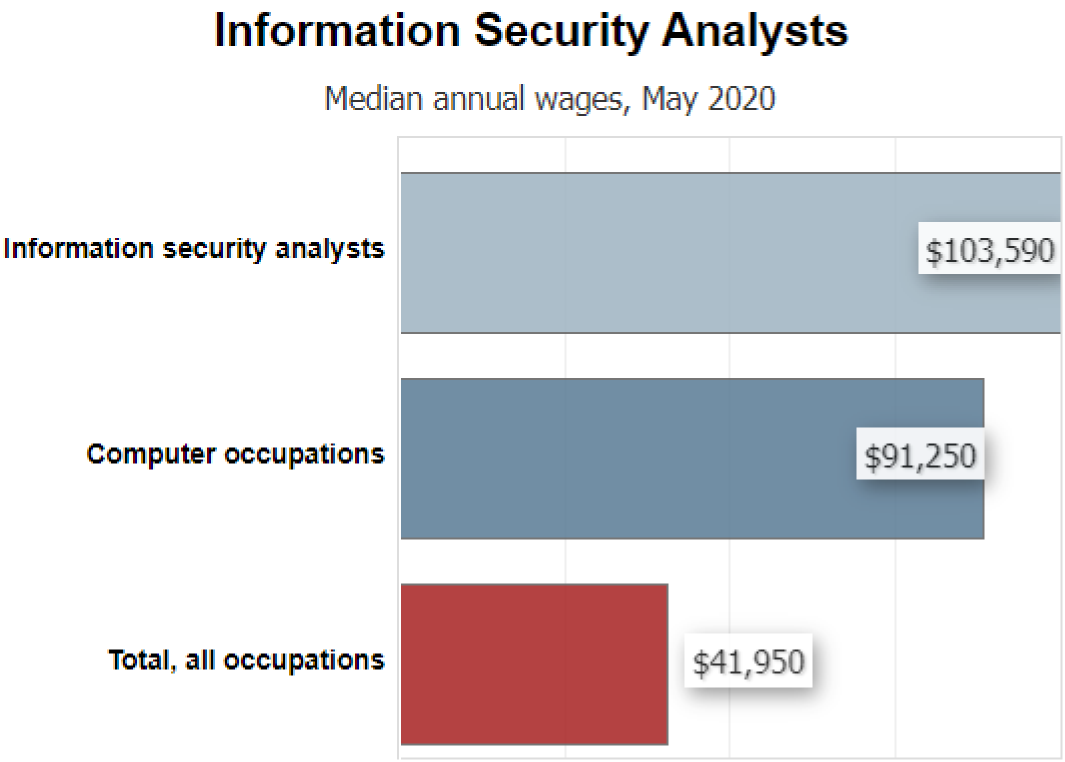


Figure 3. Median Wages of Information Security Analysts from May 2020 Compared to Computer Occupations and All Other Occupations. Source: U.S. Department of Labor, 2021.

F. BENEFITS OF AN ARMY CYBER CAREER

Throughout the career of a Cyber Security Specialist, soldiers frequently network with various civilian companies. By demonstrating that they possess the skillset and core competencies, it is quite possible for soldiers to line-up a profession following the term of their service obligation. Working in the 17C MOS for the Army allows soldiers to be relevant and highly capable resources available to these partner companies which are not available to the general business community.

Following the initial term of enlistment for a cyber security specialist; many of the three-letter organizations, (i.e., Central Intelligence Agency [CIA], Department of Homeland Security [DHS], Federal Bureau of Investigation [FBI] and National Security Agency [NSA]) or functional security administrations would be amenable to utilize their respective skills and compensate as much as $110,000 in salaries (Job Test Prep, n.d., under "Careers After the Military").

The overarching objective for the cyber security specialist remains the same. It is the specialized ability "to conduct integrated and synchronized Offensive Cyberspace Operations (OCO)," (U.S. Army Cyber School, 2020b, under "Purpose"), with the explicit intent to project supremacy while dispensing force in and through cyberspace. The Army's 17C's have a functional responsibility to pace the threat by focusing on enemy and hostile activities, competencies, and Defensive Cyberspace Operations (DCO). The end state is to be able to defend "data, networks, net-centric capabilities, and other designated systems by detecting, identifying, and responding to attacks against friendly networks, with other lethal and nonlethal actions that enable commanders to gain advantages in cyberspace and across all domains" (U.S. Army Cyber School, 2020b, under "Purpose").

G. RECRUITMENT, RE-ENLISTMENT, AND RETENTION

1. Recruitment

Not only are the costs high regarding recruit training but the overall recruit pool is significantly less than other MOSs based on the ASVAB requirements. The 17C MOS ASVAB score requirements are high for the ST and GT portions described in Chapter II Table 2. This variation of test qualification test scores is shown in Figure 4. It is important to note that the 17C MOS was not created until 2015. Data prior to 2015 is assumed to be composed of the combination of ASVAB data for the MOSs of which 17C borrowed from.

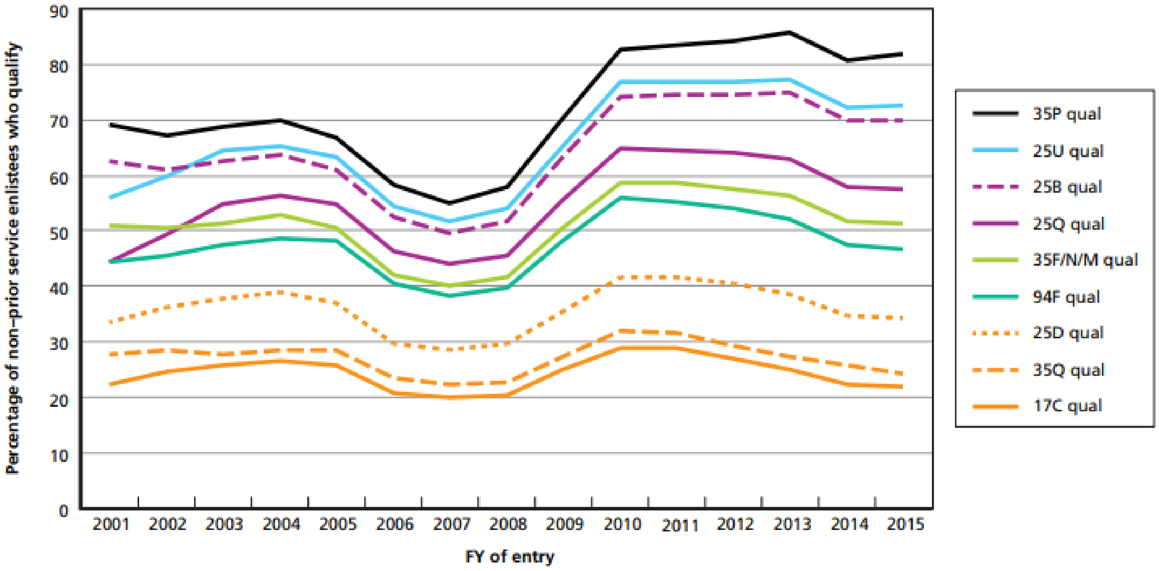


Figure 4. ASVAB Test Score Qualification Rates for Various Army MOSs. Source: Wenger et. al. (2017).

Figure 5 breaks down the percentage of recruits that meet or exceed ASVAB test scores at various intervals. Wenger et al. estimate that based on the levels of recruits meeting or exceeding the ST and GT scores for the 17C MOS in Table 2, there would be at least 10,000 soldiers who would qualify. This begs the question why is recruitment and attrition low if there are 10,000 qualifying soldiers?

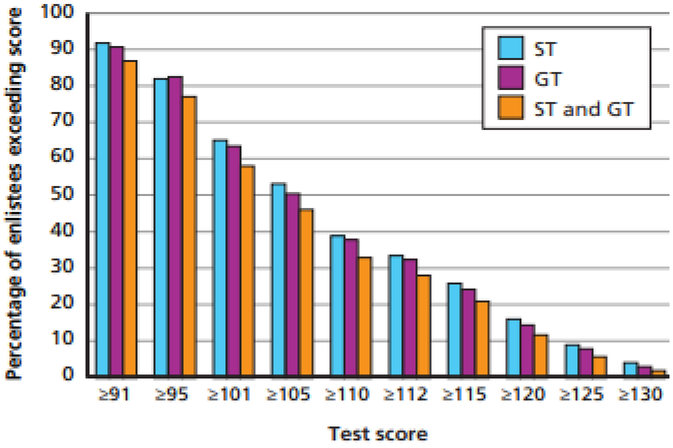


Figure 5. Percentage of Recruits that Meet or Exceed ST and GT Test Scores Ranging from 91 to Over 131. Source: Wenger et. al. (2017).

2. Reenlistment

Research completed by Wenger et. al. (2017) has shown that soldiers enlisted under the 17C MOS will tend to fulfill their first enlistment tour. After the first enlistment though, these 17C cyber trained soldiers interest fades and second term enlistment numbers begin to suffer, according to a recent RAND Corporation study (Wenger et al., 2017, pp. 6–7). Figure 6 shows that soldiers that do meet the qualifications for the 17C MOS are more likely to remain in the Army over their first enlistment term when compared to other soldiers.

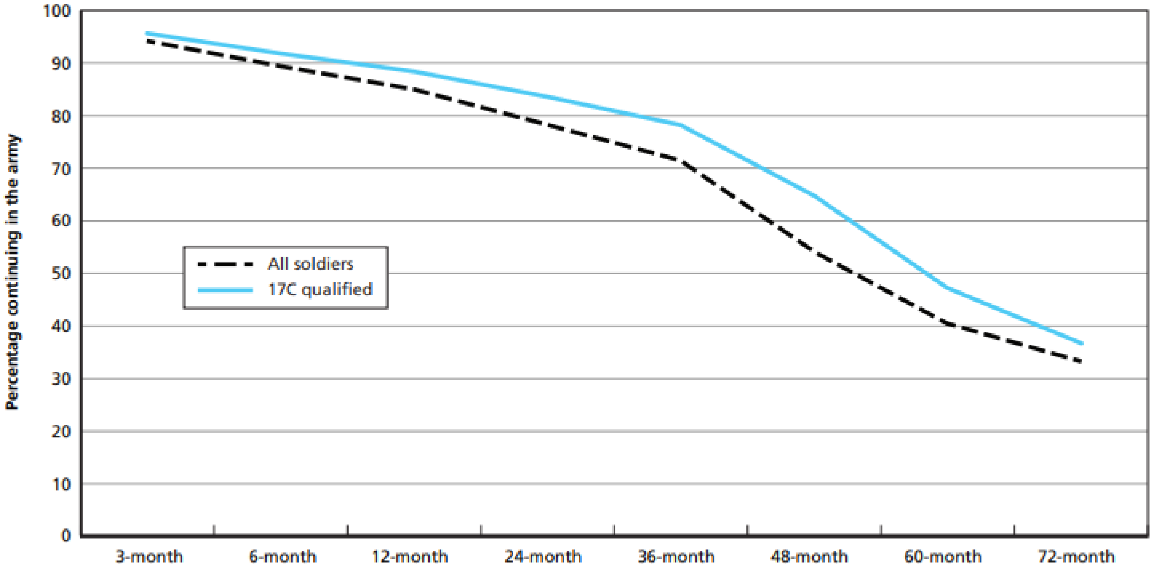


Figure 6. Length of Service Continuation for 17C MOS Qualified Soldiers Compared to Other Soldiers. Source: Wenger et. al. (2017).

"Given the very long training pipeline and the substantial costs associated with training a 17C soldier, the Army needs to understand as much as possible about the likely continuation rates to ensure there is sufficient return on its training investment," the study said (Bur, 2019, para. 2). "Soldiers who qualify for 17C are more likely than others to remain in the Army for at least 72 months (about 6 years)," (Wenger et al., 2017, pp. 2). Figure 7 shows that the reenlistment rate for 17C qualified recruits with varying service obligation periods.

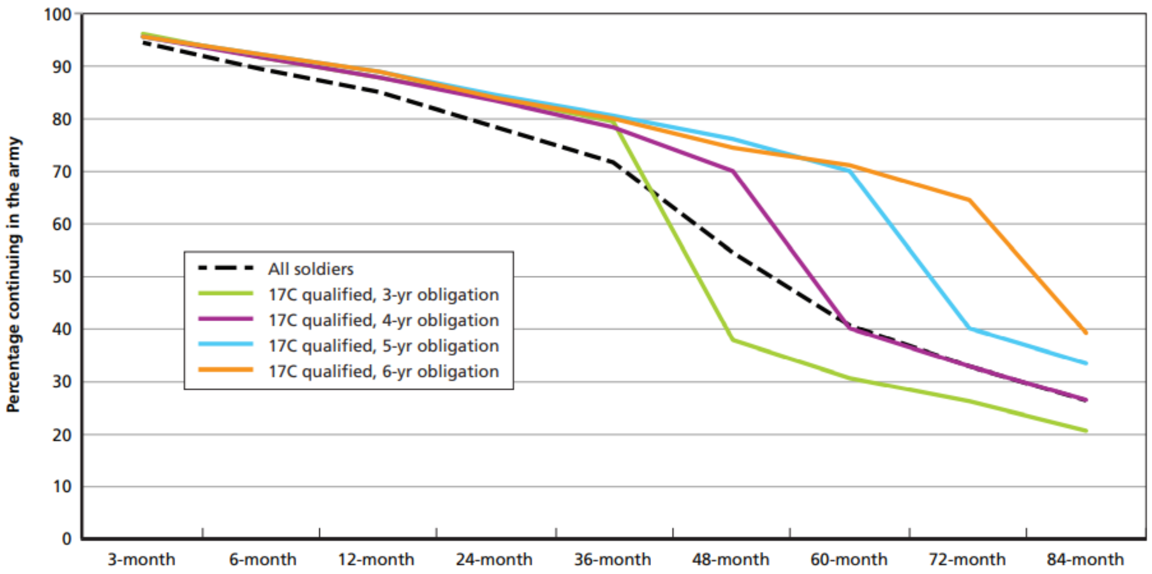


Figure 7. Reenlistment or Continuation Rates of 17C Qualified Recruits with Varying Service Term Agreements. Source: Wenger et al., 2017

Wenger et al. go on to describe Army senior leadership and their fears with the opportunities offered by the private sector how likely talented cyber specialists [17C MOS soldiers] may be lured away from continuing their military service. Additionally, she suggests "that tracking civilian compensation and hiring will play an important role in managing Army cyber occupations [in the future]," (Wenger et al., 2017, pp. 16).

3. Transition for Enlisted Personnel to MOS 17C

As a brand new MOS, the 17C program needed recruits quickly. The Army released Military Personnel (MILPER) Message 15–165 which authorized the transition of certain existing MOSs to 17C to increase its personnel levels quickly. Table 7 shows the MOSs and ranks that were converted to the new 17C MOS in 2015. These transitions were limited to three units which included 780th MI BDE (W6VAAA), the 7th Cyber Protection BDE (W6ZBAA), and the Joint Force HQ-Cyber (W6Z8AA) (MILPER, 2015, para. 2). The transition to 17C did not extend soldiers terms of service.

Table 7. 17C Transitions. Adapted from MILPER Message Number 15–165 (2015).

	From						17C	1510 UAD		
	25B	25D	35Q	35N	35V/X	29E	Total	Auth.	Delta	%
SL1	1	0	182	0	0	0	183	264	81	69
SGT	4	0	69	0	0	0	73	157	84	46
SSG	15	20	110	2	0	0	147	146	-4	102
SFC	3	49	48	0	0	0	100	106	6	94
MSG	0	6	1	0	5	0	12	32	20	37
SGM	1	0	0	0	2	1	4	7	3	57
Totals	24	75	410	2	7	1	519	709	190	73

Note that data reflects initial transitions into the 17C MOS. This data was provided by USAREC in reference to MILPER Message 15–165 (2015).

4. Selective Retention Bonus (SRB) Program

The Army can offer Selective Retention Bonus (SRB) incentive pay to highly qualified candidates across a wide variety of Primary Military Occupational Specialty (PMOS) or MOS. MILPER Message Number 20–258 outlines the details of the SRB program and which PMOSs qualify. One item to note from this MILPER message is that the PMOS must be listed as a tier 3 rating or higher to receive an SRB (MILPER, 2020, para. 4). Both 17C MOS fields are listed as tier 9 and 10 for each of the soldier ranks. The tiered ranking scale is numbered from 1 to 10 and is shown in Table 8.

Table 8. Qualifications for Lump Sum, Flat Rate Payments for 17C. Adapted from MILPER Message Number 20–258 (2020).

MOS	TAFS	SQI	ASI	Location	SL1	SGT	SSG	SFC
17C	-	-	-	-	9	9	9	9
17C	-	-	E6	780TH MI/CYBER PROT BDE	10	10	10	10

Note the following column headings are defined as Total Active Federal Service (TAFS), Skill Qualification Identifier (SQI) or Additional Skill Identifier (ASI). Location 780th MI/CYBER PROT BDE is the 780th Military Intelligence (MI) Brigade (Cyber).

Based on the tier levels in Table 8, Table 9 defines the payments sums for the PMOS regarding the Total Active Federal Service (TFAS).

Table 9. SRB Amounts Associated with the Ranks in Table 8. Adapted from MILPER Message Number 20–258 (2020).

Tier Level	Rank	12 – 23 Months	24 – 35 Months	36 – 47 Months	48 – 59 Months	60 or More Months
9	PFC	$4,800	$10,300	$16,900	$36,300	$54,200
	SPC	$5,300	$11,200	$18,400	$39,500	$59,000
	SGT	$5,800	$12,300	$20,300	$43,500	$65,000
	SSG/SFC	$6,500	$13,800	$22,700	$48,800	$72,900
10	PFC	$5,400	$11,400	$19,900	$40,300	$60,200
	SPC	$5,900	$12,400	$21,600	$43,900	$65,600
	SGT	$6,500	$13,700	$23,800	$48,400	$72,200
	SSG/SFC	$7,200	$15,300	$26,700	$54,200	$81,000

IV. ANALYSIS

A. PRIMARY RESEARCH

The primary research question of this thesis is presented in Chapter I under the Scope of Research heading. The question asks to find and identify issues regarding recruitment, retention, and sustainment the U.S. Army is experiencing with its Military Occupational Specialty (MOS) 17C career category, Cyber Operations Specialist. Data for this primary research question was collected through multiple online literature sources. Working knowledge was also collected from an author's experience working at USAREC as an Army Recruiting Guidance Counselor (ARGC) while serving in the U.S. Army. Other sources include data received directly from the United States Army Recruiting Command (USAREC) which was supplied in the form of Military Personnel (MILPER) messages. USAREC was unable to be reached for more current enlistment and retention data upon supplying the initial round of MILPER messages. These items can be found in Chapter V under Topics for Further Study to be explored when additional data is made available. Data regarding retention and sustainment was then sourced from a RAND Corporation study in 2017 covering similar topics. The conclusions drawn from the data in Chapter III were based upon multiple literature sources as well as the author's professional experience from working in the military and civilian DOD workforces as well as general knowledge of work-life balances.

- What are the Recruitment, Retention, and Sustainment Issues the U.S. Army is Experiencing within the 17C MOS?

The Introduction, Chapter I, establishes that the U.S. Army has the highest 36-month attrition rate out of all the services from fiscal year 2001 through fiscal year 2013. The author of the study that presented that data, Marrone (2020), ensured that data taken in fiscal year 2013 carries through to the recruits first term ending in March of 2017, completing a full thirty-six-month enlistment obligation. The reader then understands that there is an attrition issue with the U.S. Army in past years. Attrition is defined as "a reduction in numbers usually because of resignation, retirement, or death," (Merriam-

Webster, n.d., under "Definition of attrition item 4"). The Analysis in Chapter IV will identify attrition through the areas of recruitment, retention, and sustainment. These three areas are essential to understand first to then understand the attrition topic. What this research question does not address is the solution to recruitment and associated issues. U.S. Army recruitment has been studied in the past and is well understood by academia and the U.S. Army. The authors assume that the readers understand or can research recruitment efforts and their role in the retention and sustainment efforts. Recruitment data only pertaining to the 17C MOS was used.

a. 17C MOS Transition Program

Soldiers were pulled from other similar MOS sectors to staff the 17C program when first created in 2015. These similar MOS categories included those in Table 7 such as subsets of MOS categories 25, 29, and 35. The takeaway from Table 7 is that the initial fielding targets of the 17C MOS were not sufficient to execute the transition plan set forth by the U.S. Army. The U.S. Army was only able to fill seventy-three percent of the required 17C positions which equates to five hundred and nineteen individuals out of the required seven hundred and nine individuals. The 17C program began with a deficit of personnel.

b. Recruitment for the 17C MOS

Recruits are typically assigned a recommended MOS upon completion of the ASVAB. The ASVAB recommends a best fit MOS for candidates based on the answers provided. It should be noted that the achieved scores on the ASVAB in Table 2 to qualify for the 17C MOS are high when compared to the scores required for other MOS in the U.S. Army. A comparison of these scores is shown in Appendix A. There are only five other MOSs that require scores at or above the line scores required for the 17C MOS, which are presented in Chapter II, Background. These scores are 110 on the GT section of the exam and 112 on the ST section of the exam. 17C MOS candidates are expected to score highly on the ST and GT line scores to qualify. If the Army's potential pool of candidates for the 17C MOS is limited from the beginning, this drastically reduces the candidates that can select 17C as a MOS moving forward. It may also limit the potential pool of candidates who may score just under the thresholds but may be qualified in other topic areas pertaining to the 17C MOS. Figure 4, compiled by Wenger et. al. (2017), depicts that the 17C MOS has the least number of qualified applicants who achieve the required ASVAB scores when compared to other data driven MOS. Appendix A shows that the 25 series MOS encompasses specialized communication tasking, the 35 MOS series encompasses intelligence and cryptography, and the 94 series MOS encompasses radar and aviation-based tasking. There is some interconnectedness when analyzing these MOSs but 17C is still highly specialized and requires a large pool of potential candidates as well as increasing numbers every year with the growing cyber security threat from rival nations. Figure 5, also compiled by Wenger et. al. (2017), compares the line scores for recruits versus the percentage of recruits who meet or exceed those levels. Based on Figure 5, thirty-three percent of all recruits who take the ASVAB meet the minimum line scores for the GT, which is 110, and twenty-eight percent of all recruits meet the minimum score for the ST portion, 112, to qualify for the 17C MOS.

Other standards may disqualify potential candidates such as stringent physical fitness tests, criminal background checks, and illegal substance testing. The idea of relocating periodically through a service commitment may also reduce the number of potential applicants. If new recruits have family roots in certain areas, they may be unwilling or unable to relocate away from their home.

Without current recruitment numbers for each MOS listed here, an accurate analysis could not be drawn as to how many actual recruits choose the 17C MOS over the other MOS for which they qualify for. Based on the data provided, an analysis is completed on potential reasons for which 17C recruits chose to separate from the service after short enlistment periods.

c. Retention of 17C Soldiers

The topic of compensation should be tied into the attrition issue in a highly specialized field such as the 17C MOS. Table 4 depicts the yearly pay by rank for enlisted personnel in the U.S. Army and Table 5 depicts the monthly pay based on years of service. For a comparison on near equal experience levels for compensation, an entry level E4 with a bachelor’s degree and three years of military service is contrasted with a civilian with a bachelor's degree with three years of private sector work experience. According to Figure 2, the civilian Cyber Security Analyst I would have a compensation of $70,809 in year one. Figure 3 provides the average compensation for the other civilian 17C MOS equivalent position, an Information Security Analyst, which is listed at $103,590. Appendix B includes other civilian career choices that align closely to the roles and responsibilities that are covered under the 17C position. To simplify this comparison, an average annual median compensation for both the Cyber Security Analyst I and the Information Security Analyst was calculated to be $87,200. Accounting for an estimated two percent to three percent wage increase per year, the civilian equivalent 17C MOS position would be estimated at $91,615 in year 3. The base annual compensation of an E-4 in Table 5 with three years of experience was calculated to be $30,263 which falls between the annual compensation of two years and four years of experience. The other portion of an E-4's compensation are the allowances. This portion varies greatly depending on family status, location, and rank. Rank is already addressed, and the family status was assumed to have dependents. To find an average for the total allowance portion of an E-4's compensation, the Regular Military Compensation (RMC) Calculator was used from the Military Compensation website in the DOD. Selecting an E-4 with three years of service, married filing jointly, and working at Fort Meade, zip code 20755, provided a total compensation of $64,142 (DOD, n.d.). Removing the healthcare portion of the civilian pay as demonstrated by the U.S. Army's benefits website comparison (U.S. Army, n.d.b under "Total Compensation") using the suggested Peterson KFF Healthcare Cost Estimator normalizes the civilian compensation to be accurately compared to the U.S. Army's 17C MOS compensation. The healthcare costs were calculated to be $12,500 for a family of found, supported by an employer insurance plan, with average health and an annual income of $100,000, (Peterson KFF, n.d., under "Household Health Spending Calculator"). The total civilian compensation was found to be $79,114 and the 17C MOS total compensation was found to be $64,142. For these positions, the average compensation gap between the Army 17C position and civilian equivalent was calculated to be $14,972 per year. Total compensation is only a portion of the discussion about retention.

Wenger et. al. (2017) presents the case that the likelihood of 17C MOS soldiers reenlisting after their first thirty-six-month service agreement drops from eighty percent to sixty-five percent by forty-eight months to just under fifty percent at sixty months to a low of just under forty percent at seventy-two months. Even with this steep decline, the average 17C MOS soldier is more likely to reenlist than other soldiers in the U.S. Army. This data is presented in Figure 6. Figure 7 continues to show reenlistment rates but within the 17C MOS with varying initial service term obligations. Overall, 17C MOS soldiers are more likely to reenlist than other soldiers in other MOS categories. The one exception is with 17C soldiers who initially enlist for the thirty-six-month period. Wegner et.al. (2017) attributes this to soldiers not selecting the correct MOS from the beginning. This is also reinforced by Marrone (2020) in the RAND study completed on thirty-six-month attrition rates in the military. Soldiers enlisting for thirty-six-month service obligations may be undecided if a commitment to service is suitable, or not favorable to their desired lifestyle. Soldiers who select a service obligation with a longer term of service may already have an MOS selected and realize that they are a correct fit. Looking past thirty-six-month reenlistment rate, the concern lies with the reenlistment rate of soldiers who fulfill their sixty- or seventy-two-month service obligation. At this point, the U.S. Army has made a significant investment in these individuals, and these soldiers have had a substantial amount of field experience in the 17C MOS realm. The experience that these each of these soldiers possess at the seventy-two-month period is extremely valuable to the Army but also to the private sector. To maintain staffing levels of the 17C MOS, the U.S. Army must recognize these factors, and attempt to gain reenlistment service obligations from the soldiers through various means.

The U.S. Army realized this and began its Selective Retention Bonus (SRB) program. This program seeks to entice soldiers, who hold special skills in high demand areas, to remain in the Army through extra compensation packages and incentives. One of the documents that highlighted the SRB program for the 17C MOS was MILPER Message Number 20–258 (2020). Data from this message is included in Chapter III, Data, in Tables 8 and 9. Table 8 identifies the two areas of the 17C MOS eligible for an SRB upon reenlistment. It is important to note that the Army ranked both 17C MOS positions as tier

9 and tier 10 out of 10 tiers. Higher tiers represent higher priority MOSs in which the Army wants to maximize soldier retention. It also shows that the Total Active Federal Service (TAFS) does not have a value present. This makes the point that 17C soldiers are important to retain at any point in their career. Table 9 depicts the SRB compensation based on rank, time in service, and tier level. With increasing rank and time in service, the SRB steadily increases.

Assuming an equal distribution of the SRB over a new seventy-two-month enlistment for the maximum amount at an SSG/SFC (E-6 or E-7 according to Table 4) tier 10 for sixty months or more, this would add $13,500 on top of the total compensation per year. Using the RMC calculator from DOD (n.d.) for an E-6 with all inputs the same as the E-4 comparison, places the total regular military compensation at $79,978 per year. Adding the SRB to this would make an E-6 17C soldier's annual compensation $93,478. Finding a civilian equivalent compensation at year seven would vary greatly. One can assume a civilian may have selected a management track in the computer and information systems management career after their first five years (U.S. Bureau of Labor Statistics, 2021, under "Summary") placing their median compensation at $151,150. Subtract the estimated $17,850 in healthcare costs (Peterson KFF, n.d., under "Household Health Spending Calculator") and this places the total annual compensation of a civilian with six years of experience at $133,300. There are many civilian equivalent positions that a 17C soldier could create a career from as shown in Appendix B. These are strictly examples that were selected for calculation purposes.

B. SECONDARY AND SUPPORTING RESEARCH

The secondary and supporting research questions posed to the reader are found in Chapter I under the Scope of Research heading as an indented list. These research topics include career fields in the civilian sector that require similar skillsets to the 17C MOS, what is the overlap or gap between the 17C skillset and the civilian equivalent, additional compensation packages being offered to civilians that are not being offered to 17C soldiers, and finally, how these civilian positions are affecting the sustainment of the 17C MOS by the U.S. Army. Data for these topics were sourced from public facing websites and reports.

This data was collected and compiled in Chapter III to depict differences and similarities between the U.S. Army's 17C MOS and the civilian equivalent as well as supporting data to show the variations between the military and civilian career fields.

- What Factors are Contributing to the Transition of 17C Soldier to Private Industry?

a. What civilian cyber security occupations are similar or equal to the 17C MOS roles and responsibilities?

Appendix B was sourced from the Disabled Veterans National Foundation and serves as a resource for veterans to determine what civilian career field their MOS will fit best with. In the case of the 17C MOS, thirty-six results were returned and centered around four main categories which include Computer & Information Systems Managers, Computer Network Support Specialists, Information Security Analysts, Network & Computer Systems Administrators (Disabled Veterans National Foundation, n.d.). All listed career fields will require some or all the trainings outlined in Table 3. It is important to note that the trainings listed are applicable to both military and civilian careers. The civilian career field list in Appendix B is only one resource available to soldiers to assist with transitioning from the military into the civilian labor force. There are many options available to soldiers, but the U.S. Army's assumed preference is reenlistment which ensures the knowledge and experience remains within the 17C MOS.

b. What is the overlap or gap that exists with regards to the 17C MOS training and certification program when compared to private industry?

Upon conclusion of the research contained within this thesis, it was determined that the core training curriculum skillset for civilian IT and the 17C MOS are the same. The certifications outlined in Table 3 are recognized internationally and span both public and private sectors. Earning these certifications in either field will transition with the individual through their career. The difference is that the U.S. Army bears the cost burden for soldier where the individual may have to pay up front then be reimbursed if their employer does not cover the costs.

c. *Are private corporations offering above and beyond the compensation packages or additional trainings than what is offered by the United States Army 17C MOS?*

U.S. Army 17C compensation is outlined by rank. Soldiers may advance at a regular rate but there is eventually a cap to the compensation offered. SRBs and signing bonuses are offered to 17C soldiers but have specific limits in the amounts to which they are offered. They are also not offered yearly unless the total SRB or bonus payout is structured over the enlistment obligation period. In contrast, private industry has no set compensation structure and may be able to offer as much or as little as required to attract or retain individuals. Bonuses may be offered throughout the year with no limits to the amount. Individuals may also use multiple company offers to ensure they are receiving the best compensation package. Both the military and the private sector offer opportunities for advanced education or other certifications. Dollar amount limits may be imposed for both sectors on a yearly basis and certain academic grades may be required to receive full reimbursement for the training.

In addition to compensation, other benefits to include medical, dental, vision, retirement, paid time off and flexible working arrangements. The military, historically, offers great benefits which may not always be accounted for when new recruits are enlisted and only thinking about annual pay. Benefits will vary from private company to private company, but it is assumed that most private companies cover at least a portion of benefit costs where the U.S. Army covers the full cost. Flexible working arrangements have been gaining popularity in recent years. Due to the nature of the work conducted by the U.S. Army, in most cases, working from home or a remote location, may not be feasible. If the work falls under various classification levels, soldiers will have to work from buildings and locations that meet the security requirements. This will severely limit flexible working arrangements when compared to the private sector.

d. How are employment opportunities in the civilian IT community are impacting the retention and sustainment of 17C MOS soldiers in the Army

Benefits such as flexible schedules, in most cases, higher overall compensation packages, and unlimited growth opportunities are only a few of the value adding perks that the private sector can offer to newly retired 17C soldiers. With the history of military service, leadership, and field experience, these soldiers are extremely valuable to the private sector. In reference to the two civilian career fields that compare to the 17C MOS, both fall within the IT/cybersecurity field. The Bureau of Labor Statistics estimates that the information systems security field will grow by thirty-one percent over the next decade (U.S. Bureau of Labor Statistics, 2021, under "Job Outlook"). If the U.S. Army is considered a single company in a highly in demand and competitive career field, they need to ensure the methods for recruitment, retention and sustainment are overhauled and modernized to better align with the private sector. With the private sector offering large compensation packages, flexible work schedules, and low stress work/life balance plans, this places the U.S. Army in a highly competitive employer pool. By ensuring hiring practices and compensation offerings are innovative and competitive, this will keep their labor force fresh. It will also assist in the retainment of valuable knowledge and training to transfer it to newly minted soldiers.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS, RECOMMENDATIONS, AND TOPICS FOR FURTHER STUDY

A. CONCLUSIONS

1. Entrance Requirements

Wenger et.al. asserts, "In the case of 17C, the vast majority of soldiers who enter the Army do not meet the requirements to serve in the MOS," (2017, pp. 5). That is due to the high General Technical (GT) and Skilled Technical (ST) scores required for the Military Occupational Specialty (MOS) of 17C. Wenger et. al. further states, "MOS, 17C, has stringent entrance criteria; in particular, the required scores on the ST and GT line scores mean that only a fraction of new enlistees are qualified to enter the MOS," (2017, pp. 15). Moreover, Wenger et al. further avows "to build its 17C workforce, the Army is pulling talent from within the Army as well as growing new talent from those entering the Army," (2017, pp. 3). It is important to know that people are our most important and significant asset. The sustainment of our 17C MOS is necessary for the Army to seek further measures to incentivize and increase its overall retention. "The 17C Soldier must have a SECRET clearance to apply but they must meet interim TOP SECRET (TS) Sensitive Compartmented Information (SCI) access eligibility requirements prior to course attendance and to be awarded MOS, then final adjudication to maintain MOS," (U.S. Army Cyber School, 2020b, under "Minimum Requirements").

2. Specialized Training

"The specialized training provided to Army cyber personnel is likely to be of value in the civilian world" (Wenger et al., 2017, pp. 15). Wegner et al. further declares that "InfoSec analysts command relatively high salaries, and a substantial proportion of civilian workers in this occupation are veterans" (2017, pp. 15). The U.S. Army Cyber Security specialist receives unconventional training. "Starting with extensive technical preparation in everything from database design to computer networking to communications systems, skills continue to be enhanced through classroom and on-the-job instruction," (Today's Military, n.d., under "Military Training"). The two phased training course encompassing a combination of 45 weeks (about 10 and a half months) of deliberate instruction and certifications establishes the baseline for a successful career of supporting and defending the Constitution of the United States.

3. Benefits

With the multitude of benefits offered by the U.S. Army to soldiers overall in the form of a lucrative career there are no comparison to that which is offered by civilian employers. Some of the benefits include free medical and dental coverage for the service members and their dependents, 30 days (about 4 and a half weeks)' vacation per year, (i.e., which does not include 11 major holidays), unlimited sick leave in comparison to the average 14 days (about 2 weeks) that an entry level civilian would receive, and an option to select up to $400,000 in Service Group Life Insurance (SGLI). Despite the benefits which can be monetized for 17C soldiers to show the overarching value of their earnings, "Retention efforts may be seriously hampered by the perceptions young enlisted might have regarding their civilian opportunities outside the Army," (Wenger et al., 2017, pp. 15).

4. Reasons for Attrition

Along with the tough, physically demanding standards as an entry criterion, it is evident that many recruits would not fit into this military occupational specialty. There are, nonetheless, factors that cause recruits to not complete their respective term of enlistment beyond just simply exiting the U.S. Army. The fact is, "more than one-quarter of soldiers fail to complete at least 36 months (about 3 years) of their contract for reasons classified as failure to adapt," (Wenger et al., 2017, pp. 15). There are also related civilian careers that can entice veterans to pursue them such as: Information Security Analysts coupled with Network and computer Systems Administrators. Primarily the resources and skills acquired while on active duty is one of the main reasons for attrition. Employment and training while in the U.S. Army, "can serve as the foundation for a later civilian career," (U.S. Army Recruiting, 2018).

5. Geographical Locations

Army Cyber Operations Specialist following Basic Training (BT) and Advanced Individual Training (AIT) are stationed in limited duty stations and locations, which are as follows:

- Fort Belvoir, VA.
- Fort Gordon, GA.
- Fort Huachuca, AZ.
- Fort Shafter, HI.
- Wiesbaden Germany.
- Camp Arifjan, Kuwait.
- Camp Walker.

At the above-mentioned duty stations, 17C Soldiers spend time working with civilians where collectively they "Conduct integrated and synchronized Offensive Cyberspace Operations (OCO) intended to project power by the application of force in and through cyberspace by targeting enemy and hostile adversary activities and capabilities, and Defensive Cyberspace Operations (DCO) to protect data.," (U.S. Army Cyber School, 2020b, under "Purpose"). Duty location is a significant factor regarding soldiers and retention. As a former Army Recruiting Guidance Counselor (ARGC) one of the incentives that was offered was guaranteed station of choice.

B. RECOMMENDATIONS

After reviewing data and forming conclusions, U.S. Army senior leaders should consider petitioning Congress for additional support through both monetary and non-monetary incentives which include but are not limited to:

- Review current pay levels and comparing them to similar career fields found in the private sector. Pay rates could be adjusted as deemed necessary.

- Consider a guaranteed station of choice.

- Offer a potential minimum of 6 years initial enlistment obligation.

- Offer an optional maximum of 10 years initial enlistment obligation.

- Review the Written Bonus Agreement (WBA) and make current to reflect a potential increase for accommodating the Senior Enlisted Soldiers in MOS 17C (Cyber Operations Specialist), at the grades of Staff Sergeant (E-6) through Sergeant Major (E-9). Losing soldiers in these high grades significantly impacts the institutional knowledge required for sustainment in the 17C MOS. The average 17C (Cyber Operations Specialist) soldier who is completing their initial term of service (i.e., six years) should have reached the grade of SGT - SSG. The incentive in the amount of WBA should be reviewed and compared to the salary that is being offered by industry and thus serve to bridge the gap between industry and the Army for retention of the MOS.

- Consider increasing the number of Geographical locations throughout the multitude of military bases both CONUS and OCONUS to create opportunities for travel for soldiers and an incentive toward the Guaranteed Station of Choice opportunities.

- Study the implementation of a meritorious promotion program, as shown in Table 10, whereby upon re-enlistment a soldier can be promoted to prespecified ranks. This would allow for potential talent to be immediately injected in the promotion pipeline and close the pay gap between entry-level soldiers and civilian counterparts.

Table 10. Recommended Meritorious Promotion Program (MPP) for New Enlistees.

Training Obtained Prior to Enlistment into the Army	Corresponding Promotion with Individual Certification or Combined
CompTIA A+	Promotion to E-2
CompTIA Network+	Promotion to E-2
CompTIA Security+	Promotion to E-2
Certified Ethical Hacker (CEH)	Promotion to E-2
CompTIA A+ CompTIA Network+ CompTIA Security+ Certified Ethical Hacker (CEH)	Promotion to E-3
Certified Information Systems Security Professional (CISSP)	Promotion to E-4
CISCO Certified Networking Associate (CCNA)	Promotion to E-4

- Implement a Meritorious Promotion Program (MPP), which would provide an outstanding opportunity for17C Soldiers that possess the potential to perform their duties of increased responsibility. The Army should be incredibly careful not to utilize this program as a reward but instead an incentive. The program for 17C soldiers should be solely for those who demonstrate the ability to perform the duties of a higher grade. This program should be available to Sergeant E-5, Staff Sergeant E-6, and Sergeant First Class E-7. Table 11 recommends the MPP insertion points for E-5 through E-7 by grade. A Department of the Army for 4187 can be utilized to initiate the MPP process.

Table 11. Recommended MPP Insertion Points for E-5 through E-7

Meritorious Promotion Program (MPP)	**MPP Grade**
Company Commander’s Recommendation	Promotion to E-5
Battalion Commander’s Recommendation	Promotion to E-6
Brigade Commander’s Recommendation	Promotion to E-7

C. TOPICS FOR FURTHER STUDIES

As time rapidly concluded for the completion of this thesis, the authors included other topic areas pertaining to the research conducted within. For further studies, it would be recommended that a more in-depth review be conducted to include all military service branches and DOD civilian commands to determine the attrition rate of related cyber fields. This may assist the DOD to determine how to continue to strengthen its cyber operations and remain at the forefront of defense and offensive cyber activities. The authors would also recommend including DOD contractor support in the cyber field as well. Many commands are supported by DOD contractors who work alongside of DOD civilians and DOD military. The research would determine the attrition rate of these contractor personnel as well as the organic cyber field knowledge left behind with the DOD once the contractor personnel rotate out or are replaced under another contract.

Another broad topic would include researching any DOD training pipelines that start in secondary education. Military Reserve Officer Training Corps (ROTC) or tuition reimbursement programs for civilians could be studies to determine the rate of recruitment then how long the service obligations are after the obligation is fulfilled. Would these individuals remain with the DOD, or do they tend to exit soon after the obligation is fulfilled?

Lastly, a human factors study could be conducted across the DOD. This would include a survey to determine why civilian DOD employees or soldiers have left previous roles within the DOD and what factors influenced their decisions to move? Factors such as management, location, workload, and stress levels could be included. The survey would also inquire about prior DOD or private sector employment to attempt to construct and overall picture of the makeup of the cyber workforce within the DOD and predict attrition in sectors that important. With this knowledge, the DOD could adjust recruitment and retention policies and procedures to maximize benefits and become a direct competitor to the top technology firms in the private sector. It would also ensure a long-term workforce capable of handling present and future cyber related threats facing the United States.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A ASVAB MINIMUM LINE SCORES FOR VARIOUS ARMY MOS POSITIONS

Table 12. Army ASVAB Line Scores. Source: Military.com (2021)

MOS	ARMY JOB TITLE	Minimum ASVAB Line Scores
09C	Trainee language	AFQT 21–30, ECLT 40 - 74, AO:54
09L	Interpreter/translator	ECLT:50
09S	U.S. Army commissioned officer candidate	GT:110
09W	Warrant officer candidate	GT:110
11B	Infantryman	CO:87
11C	Indirect fire infantryman	CO:87
11X	Infantry enlistment option	CO:87
12B	Combat engineer	CO:87
12C	Bridge crewmember	CO:87
12D	Driver	GM:98 & GT:107 & ST:106
12K	Plumber/Utilitiesman	GM:88
12M	Firefighter	GM:88
12N	Horizontal construction engineer	GM:90
12P	Prime power production specialist	GT:110 & EL:107 & ST:107
12Q	Transmission and distribution specialist	EL:93
12R	Interior electrician	EL:93
12T	Technical engineer specialist	ST:101
12V	Concrete and asphalt equipment operator	GM:88
12W	Carpentry and masonry specialist	GM:88
12Y	Geospatial engineer	GT:100 & ST:100
13B	Cannon crewmember	FA:93

13D	Field artillery tactical data systems specialist	FA:93
13F	Fire support specialist	FA:96
13J	Fire control specialist	FA:93
13M	High mobility artillery rocket system (HIMAR)	OF:95
13P	Multiple launch rocket system operations/fire direction specialist	FA:96
13R	Field artillery fire-finder radar operator	SC:98
13S	Field artillery surveyor	ST:95
13T	Field artillery surveyor/meteorological crewmember	EL:93
13W	Field artillery meteorological crewmember	EL:95
13Z	Field artillery senior sergeant	N/A
14E	Patriot fire control ENH oper/maint	MM:104
14G	Battle management system operator	MM:99 & GT:98
14H	Air defense enhanced early warning system operator	MM:99 & GT:99
14P	Air & missile defense (AMD) crewmember	OF:95
14T	PATRIOT launching station enhanced operator/maintainer	OF:95
14Z	Air defense artillery senior sergeant	N/A
15B	Aircraft powerplant repairer	MM:104
15D	Aircraft Powertrain Repairer	MM:104
15E	Unmanned aircraft systems repairer (UAS SYS REP)	EL:93 &MM:104
15F	Aircraft electrician	MM:104
15G	Aircraft structural repairer	MM:104
15H	Aircraft pneudraulics repairer	MM:104
15N	Avionic mechanic	EL:93
15P	Aviation operations specialist	ST:91
15Q	Air traffic control operator	ST:101
15R	AH-64 attack helicopter repairer	MM:99
15T	UH-60 helicopter repairer	MM:104
15U	CH-47 helicopter repair	MM:104

15W	Unmanned aerial vehicle (UAV) Operator	SC:102
15Y	AH-64D Armament / Electrical / Avionics Repairer	MM:105 & EL:100
17C	Cyber Operations Specialist	GT:110 & ST112
18X	Special Forces Recruit	GT:110 & SC:100
19D	Cavalry Scout	CO:87
19K	M1 Armor Crewman	CO:87
25B	Information Technology Specialist	ST:95
25C	Radio Operator	EL:98 & SC:98
25D	Cyber Network Defender	GT:105 &ST:105
25L	Cable System Installer/Main	89:EL & SC:89
25M	Multimedia Illustrator	ST:95 & EL:95
25N	NODAL Network System Operator	EL:102 & SC:105
25P	Microwave System Operator/Maintainer	EL:107
25Q	Multichannel Transmission Systems Operator - Maintainer	EL:98 & SC:98
25R	Visual Information Equipment Operator - Maintainer	EL:107
25S	Satellite Commo System Operator/Maintainer	EL:117
25U	Signal Support System Specialist	EL:93 & SC:92
25V	Combat Documentation / Production Specialist	ST:91 & EL:93
27D	Paralegal specialist	CL:105
31B	Military police	ST:91
31D	Criminal investigation special agent	ST:107 & GT:110
31E	Interment/resettlement specialist	ST:95
31K	Military working dog handler	ST:91
35F	Intel analyst	ST:101
35G	Geospatial intelligence imagery analyst	ST:101
35L	Counterintelligence agent	ST:101
35M	Human intelligence collector	DLAB:107
35N	Signal intel analyst	ST:112

35P	Cryptologic linguist	ST:91 & DLAB:107
35Q	Cryptologic network warfare specialist	ST:112 & ICLT:60
35S	Signal collector/analyst	ST:101
35T	Military intelligence systems maintainer/integrator	ST:112
36B	Finance management technician	CL:101
37F	Psychological operations specialist	GT:107
38B	Civil affairs specialist	GT:107
42A	Human resource specialist	GT:100 & CL:90
46Q	Public affairs specialist/journalist	GT:107
46R	Broadcast journalist	GT:107
51C	Acquisition, logistics & technology contracting NCO	GT:110
56M	Religious affairs specialist	CL:90
68A	Biomedical equipment specialist	EL:107
68B	Orthopedic specialist	ST:101 & GT:107
68C	Practical nursing specialist	ST:101 & GT:107
68D	Operating room specialist	ST:91
68E	Dental specialist	ST:91
68F	Physical therapy specialist	ST:101 & GT:107
68G	Patient administration specialist	CL:90
68H	Optical laboratory specialist	GM:98
68J	Medical logistics specialist	CL:90
68K	Medical laboratory specialist	ST:106
68L	Occupational therapy specialist	ST:101 & GT:107
68M	Nutrition care specialist	OF:95
68N	Cardiovascular specialist	ST:101 & GT:107
68P	Radiologist specialist	ST:106
68Q	Pharmacy specialist	ST:95
68R	Veterinary food inspection specialist	ST:95

68S	Preventive medicine specialist	ST:101
68T	Animal care specialist	ST:91
68U	Ear, nose and throat specialist	ST:101 & GT:107
68V	Respiratory specialist	ST:102
68W	Combat medic specialist	ST:101 & GT:107
68X	Mental health specialist	ST:101
68Y	Eye specialist	ST:101 & GT:107
74D	Chemical operations specialist	ST:100
88H	Cargo specialist	GM:88
88K	Watercraft operator	MM:99
88L	Watercraft engineer	MM:99
88M	Motor transport operator	OF:85
88N	Transportation management coordinator	CL:95
88P	Locomotive rep	MM:97
88T	Railway section repairer (R)	MM:87
88U	Railway operations crewmember (R)	MM:92
89A	Ammunitions stock control	ST:91
89B	Ammunitions specialist	ST:91
89D	Explosive ordnance disposal specialist (EOD)	GM:105
91A	M1 Abrams tank system maintainer	MM:88 & GT:85 or MM:99
91B	Light-wheel vehicle mechanic	MM:87 & GT:85 or MM:92
91C	Utilities equipment repair/heating & air	GM:98 or GM:88 & GT:83
91D	Power generation equipment repair	GM:98 or GM:88 & GT:88
91E	Allied trade specialist	GM:88 & GT:95 or GM:98
91F	Small arms/towed artillery repair	GM:93 or GM:88 & GT:85
91G	Fire control repair	EL:93 & GM:88 or EL:98

91H	Track vehicle mechanic	MM:87 & GT:85 or MM:92
91J	Quartermaster & chemical equipment repair	MM:87 & GT:85 or MM:92
91L	Construction equipment repair	MM:87 & GT:85 or MM:92
91M	Bradley fighting vehicle system maintainer	MM:88 & GT:92 or MM:99
91P	Artillery mechanic	MM:88 & GT:88 or MM:99
91S	Stryker systems maintainer	MM:87 & GT:85 or MM:92
92A	Automated logistical specialist	CL:90
92F	Petroleum laboratory specialist	CL:86 & OF:85
92G	Food service specialist	OF:85
92L	Petroleum laboratory specialist	ST:91
92M	Mortuary affairs specialist	GM:90
92R	Parachute rigger	GM:90 & CO:90
92S	Shower, laundry & clothing repair specialist	GM:84
92W	Water treatment specialist	GM:88
92Y	Unit supply specialist	CL:90
94A	Land combat electronic missile system repairer	EL:102
94D	Air traffic control equipment repair	EL:102
94E	Radio & communication security repair	EL:102
94F	Computer detection systems repair	EL:102
94H	Test, measurement and diagnostic equipment (TMDE) maintenance sup spec	EL:107
94M	Radar repairer	EL:107
94P	MLRS repairer	EL:93
94R	Avionic & survivability equipment repairer	EL:98
94S	Patriot system repairer	EL:107

94T	Avenger system repair	EL:98
94Y	Integrated family of test equipment operator	EL:107
96B	Intelligence analyst	ST:105
96D	Imagery analyst	ST:95
96H	Common ground station operator	SC:95 & ST:105
96R	Ground surveillance systems operator	EL:85 & SC:95
96U	Tactical unmanned aerial vehicle operator	SC:105
96Z	Intelligence senior sergeant	N/A
97B	Counterintelligence agent	ST:105
97E	Human intelligence collector	ST:95
97L	Translator/interpreter (R)	ST:95
97Z	Counterintelligence/human intelligence senior sergeant	N/A
98C	Signals intelligence analyst	ST:105
98G	Cryptologic linguist	ST:95
98H	Communications locator/interceptor	ST:95
98J	Electronic intelligence interceptor/analyst	ST:105
98K	Signals collection/identification analyst	ST:95
98XL	Signals/foreign language enlistment option	-
98Z	Signals intelligence senior sergeant	N/A

Note that the Army line scores are defined by the following two letter codes Army Line Scores:

CO -- Combat: AR+CS+AS+MC

EL -- Electronics: GS+AR+MK+EI

FA -- Field artillery: AR+CS+MK+MC

GM -- General maintenance: GS+AS+MK+EI

GT -- General technical: VE+AR

MM -- Mechanical maintenance: NO+AS+MC+EI

OF -- Operators and food: VE+NO+AS+MC

SC -- Surveillance and communications: VE+AR+AS+MC

ST -- Skilled technical: GS+VE+MK+MC

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B OTHER CIVILIAN CAREERS THAT ALIGN WITH 17C ROLES AND RESPONSIBILITIES

Table 13. MOS 17C Civilian Equivalent Careers. Source: Disabled Veterans National Foundation (n.d.).

Civilian Occupation Title	**Job Categories**	**Branch**
Application Development Director	Computer & Information Systems Managers	Army (MOS)
Computing Services Director	Computer & Information Systems Managers	Army (MOS)
Data Processing Manager	Computer & Information Systems Managers	Army (MOS)
Information Systems Director (IS Director)	Computer & Information Systems Managers	Army (MOS)
Information Systems Manager (IS Manager)	Computer & Information Systems Managers	Army (MOS)
Information Systems Supervisor (IS Supervisor)	Computer & Information Systems Managers	Army (MOS)
Information Technology Director (IT Director)	Computer & Information Systems Managers	Army (MOS)
Information Technology Manager (IT Manager)	Computer & Information Systems Managers	Army (MOS)
MIS Director (Management Information Systems Director)	Computer & Information Systems Managers	Army (MOS)
Technical Services Manager	Computer & Information Systems Managers	Army (MOS)
Computer Network Specialist	Computer Network Support Specialists	Army (MOS)
IT Consultant (Information Technology Consultant)	Computer Network Support Specialists	Army (MOS)
Network Specialist	Computer Network Support Specialists	Army (MOS)
Network Support Specialist	Computer Network Support Specialists	Army (MOS)
Network Technical Analyst	Computer Network Support Specialists	Army (MOS)
Network Technician	Computer Network Support Specialists	Army (MOS)
Personal Computer Network Analyst	Computer Network Support Specialists	Army (MOS)

Civilian Occupation Title	**Job Categories**	**Branch**
Systems Specialist	Computer Network Support Specialists	Army (MOS)
Information Security Officer	Information Security Analysts	Army (MOS)
Information Security Specialist	Information Security Analysts	Army (MOS)
Information Systems Security Analyst	Information Security Analysts	Army (MOS)
Information Systems Security Officer (ISSO)	Information Security Analysts	Army (MOS)
Information Technology Security Analyst (IT Security Analyst)	Information Security Analysts	Army (MOS)
Information Technology Specialist	Information Security Analysts	Army (MOS)
Network Security Analyst	Information Security Analysts	Army (MOS)
Security Analyst	Information Security Analysts	Army (MOS)
Systems Analyst	Information Security Analysts	Army (MOS)
Information Analyst	Network & Computer Systems Administrators	Army (MOS)
Information Systems Manager (IS Manager)	Network & Computer Systems Administrators	Army (MOS)
Information Technology Specialist (IT Specialist)	Network & Computer Systems Administrators	Army (MOS)
LAN Specialist (Local Area Network Specialist)	Network & Computer Systems Administrators	Army (MOS)
Local Area Network Administrator (LAN Administrator)	Network & Computer Systems Administrators	Army (MOS)
Network Administrator	Network & Computer Systems Administrators	Army (MOS)
Network Coordinator	Network & Computer Systems Administrators	Army (MOS)
Network Manager	Network & Computer Systems Administrators	Army (MOS)
Systems Administrator	Network & Computer Systems Administrators	Army (MOS)

This table shows potential categories based on similar skill sets possessed by the 17C soldiers, but this list is not inclusive of all positions available to 17C upon separating from the service

LIST OF REFERENCES

ASM Educational Center. (n.d.). *Cisco CCNA routing & switching boot camp.* Retrieved July 30, 2021, from https://asmed.com/course/cisco-ccna-boot-camp/

Bur, J. (2019, September 19). *Army struggles with re-enlistment of cyber talent.* MeriTalk. https://www.meritalk.com/articles/army-struggles-with-re-enlistment-of-cyber-talent/

Cisco. (n.d.). *CCNA certification and training program*. Retrieved August 1, 2021, from https://www.cisco.com/c/dam/en_us/training-events/certifications/associate/ccna-at-a-glance.pdf

CompTIA. (n.d.a). *What is compTIA A+ certification*. Retrieved August 28, 2021, from https://www.comptia.org/faq/a/what-is-comptia-a-certification

CompTIA. (n.d.b). *Why is cybersecurity important.* Retrieved July 5, 2021, from https://www.comptia.org/content/articles/why-is-cybersecurity-important

Cybersecurity Education (n.d.). *How to earn the CISSP credential.* Retrieved August 1, 2021, from https://www.cybersecurityeducation.org/certifications/cissp/

Disabled Veterans National Foundation. (n.d.). *Military to civilian occupation translator DVNF national job board*. Retrieved August 19, 2021, from https://jobs.dvnf.org/military-to-civilian-occupation-translator/

DOD. (n.d.). *Regular military compensation (RMC) calculator*. Retrieved August 19, 2021, from https://militarypay.defense.gov/Calculators/RMC-Calculator/

Evans, C., & Smith, C. (October 2019). *Beyond obfuscation: The defense industry's position within federal cybersecurity policy.* National Defense Industrial Association (NDIA) Policy Department. https://www.ndia.org/media/sites/ndia/policy/documents/cyber/beyond-obfuscation_final.ashx?la=en

Garamone, J. (2018, February 13). *Cyber tops list of threats to U.S.* U.S. Department of Defense (DOD).https://www.defense.gov/Explore/News/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says/

Gorman, S. et. al. (2009, June 24) Military command is created for cyber security. *The Wall Street Journal.* https://www.wsj.com/articles/SB124579956278644449

Iqbal, J. (2021, March 22). *CISSP certification cost – 3 components of the CISSP cost.* Master of Project Academy Blog. https://blog.masterofproject.com/cissp-certification-cost/

Job Test Prep. (n.d.). *U.S. Army cybersecurity: What you need to know.* Retrieved July 30, 2021, from https://www.jobtestprep.com/army-cybersecurity-test

Kaspersky. (2021, April 26). *What is cyber security?* https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Konkel, F. (2018, January 11). *Pentagon thwarts 36 million email breach attempts daily*. Nextgov. https://www.nextgov.com/cybersecurity/2018/01/pentagon-thwarts-36-million-email-breach-attempts-daily/145149/

Kyzer, L. (2021, April 14). *How long does it take to process a security clearance—Q2 2021 update.* Clearance Jobs. https://news.clearancejobs.com/2021/04/14/how-long-does-it-take-to-process-a-security-clearance-q2-2021-update/

Lopez, J Jr et al. (2010). Maximizing the DOD return on investment in cyberspace professionals. *IANewsletter, Volume 13* (Number 3), pages 16 - 20.

Marrone, J. (2020). *Predicting 36-month attrition in the U.S. military* (RR-4258-OSD). RAND Corporation. https://www.rand.org/pubs/research_reports/RR4258.html

Merriam-Webster. (n.d.). Attrition. In *Merriam-Webster.com dictionary*. Retrieved August 18, 2021, from https://www.merriam-webster.com/dictionary/attrition

Microsoft. (n.d.). *What is IoT (Internet of Things)?* Microsoft Azure. Retrieved July 20, 2021, from https://azure.microsoft.com/en-us/overview/internet-of-things-iot/what-is-the-internet-of-things/

Military Benefits. (2021, April 13). *2021 Military pay charts*. Military.com. (2021, April 15). ASVAB Scores and Army Jobs. https://www.military.com/join-armed-forces/asvab/asvab-and-army-jobs.html

Military Personnel (MILPER). (2015, June 2). *Transition strategy for enlisted personnel to MOS 17C.* [Memorandum]. Department of the Army. Message Number 15–165.

Military Personnel (MILPER). (2020, August 08). Selective retention bonus (SRB) program. [Memorandum]. Department of the Army. Message Number 20–258.

Myers, N. (2021, February 11,). Cyber security: Cyber crime, attacks and terrorism. [Paper Presentation]. Old Dominion University (ODU) United Nations (UN) Day 2020, Norfolk, VA. https://www.odu.edu/content/dam/odu/offices/mun/docs/1st-cyber-attacks.pdf.

Obama, B. (2014, September 30). *Presidential proclamation—National cybersecurity awareness month, 2014.* The White House. https://obamawhitehouse.archives.gov/the-press-office/2014/09/30/presidential-proclamation-national-cybersecurity-awareness-month-2014

ONLC Training Centers. (n.d.). *CompTIA security+ certification training course outline.* https://www.onlc.com/outline.asp?ccode=xsp601

Pay and Allowances of the Uniformed Services, 37USC403. (2013, January 1). https://uscode.house.gov/view.xhtml?req=37+USC+403&f=treesort&fq=true&num=212&hl=true&edition=prelim&granuleId=USC-prelim-title37-section403

Peterson KFF. (n.d.). Household Health Spending Calculator. *Peterson-KFF Health System Tracker*. https://www.healthsystemtracker.org/household-health-spending-calculator/

Piha, E. (2021, January 19). *Army cyber operations specialist (MOS 17C).* Operation Military Kids. https://www.operationmilitarykids.org/army-cyber-operations-specialist-mos-17c/

Jackson, P. (September 22, 2020). *How much does the CEH exam (really) cost?* Quickstart. https://www.quickstart.com/blog/how-much-ceh-exam-cost/

Salary.com. (2021, June 28). *Entry level cyber security analyst salary.* Salary.Com. Retrieved July 30, 2021, from https://www.salary.com/research/salary/posting/entry-level-cyber-security-analyst-salary

Smith, S. (2019, June 25). *What is the military medical PULHES grading system?* The Balance Careers. https://www.thebalancecareers.com/military-physical-profile-serial-system-4057768

Study.com. (2021, April 11). *CompTIA certification: Program overview.* https://study.com/articles/CompTIA_Certification_Program_Overview.html

TAOnline. (2021, January). *Security clearance information and jobs—hiring cleared people.* https://veteranresources.taonline.com/securityclearances/hiring-cleared-people

Today's Military. (n.d.). *Cyber security specialists*. Retrieved August 21, 2021, from https://www.todaysmilitary.com/careers-benefits/careers/cyber-security-specialists

U.S. Army. (2010, October 1). *Army establishes army cyber command.* https://www.army.mil/article/46012/army_establishes_army_cyber_command

U.S. Army. (n.d.a). *Timeline of army cyber command.* Army Cyber. Retrieved July 30, 2021, from https://www.goarmy.com/army-cyber/timeline-of-army-cyber.html

U.S. Army. (n.d.b). *Military compensation: Total military pay & benefits*. Goarmy.Com. https://www.goarmy.com/benefits/total-compensation.html

U.S. Army. (2019, January 30). *Army pay chart & army base pay – active duty.* https://www.goarmy.com/benefits/money/basic-pay-active-duty-soldiers.html

U.S. Army Cyber School. (2020a, July 31). *What is the cyber school?* Retrieved July 30, 2021, from https://cybercoe.army.mil/CYBERSCH/about.html

U.S. Army Cyber School. (2020b, July 31). *Cyber operations specialist (17C).* Retrieved July 30, 2021, from https://cybercoe.army.mil/CYBERSCH/COURSES/17c_cyber_operations_specialist.html

U.S. Army Recruiting. (2018, January 23). *MOS 17C cyber operations specialist*. https://www.youtube.com/watch?v=ev2j6KFZ-Ys

U.S. Bureau of Labor Statistics. (2021, June 2). *Computer and information systems managers*. https://www.bls.gov/ooh/management/computer-and-information-systems-managers.htm

U.S. Department of Labor. (2021, April 9). *Information security analysts: Occupational outlook handbook*. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Wenger, J. W., O'Connell, C., & Lytell, M. C. (2017). *Retaining the Army's cyber expertise* (RR-1978-A). RAND Corporation. https://doi.org/10.7249/RR1978.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California