REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
30-03-2021	Master of Military Studies (MMS) thesis	AY 2020-2021

4. TITLE AND SUBTITLE
CYBER AUXILIARY FOR TACTICAL SOF OPERATIONS

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Giraldo, Jorge E. (CIV)

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The proliferation and advancement of digitally based technologies has created shortfalls within DOD and Special Operations Forces (SOF) for filling key skilled cyber talent workforce positions. SOF and the Intelligence Community (IC) would benefit from having access to dedicated cyber specialists embedded within deployed SOF teams to handle extracting, organizing, sorting, and sending relevant data for timely analysis back to the United States. SOF needs the ability to positively identify and attribute an individual's identity to gain knowledge into threat actor planning through collected data at rest. The US Government and DOD must adapt to new ways of evaluating talent and reinvent both military and civilian positions to take advantage of the intelligence opportunities that SOF's collected data provides. Furthermore, the incorporation of Artificial Intelligence (AI) technologies for triaging and organizing the vast amounts of data collected from the battlefield by SOF would lessen the workloads for the Intelligence community to produce timely intelligence products. This thesis highlights talent shortfalls within SOF and provides suggestions for finding and retaining the scarce cyber talent as well as speed up the production of intelligence products.

15. SUBJECT TERMS
Special Operations Forces (SOF), Intelligence Community (IC), Artificial Intelligence (AI), Cyber Specialists, Sensitive Site Exploitation, Cyber operators, Cyberspace, Talent recruitment, Talent management, Talent retention, Document and Media Exploitation (DOMEX).

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
Unclass	Unclass	Unclass	UU		19b. TELEPHONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

CYBER AUXILIARY FOR TACTICAL SOF OPERATIONS

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Mr. Jorge E. Giraldo

AY 2020-21

MMS Mentor Team and Oral Defense Committee Member:
Dr. Brandon Valeriano
Approved: _____
Date: 3/27/21

MMS Mentor Team and Oral Defense Committee Member:
Mr. Jeremy Glauber
Approved: _____
Date: 4/12/21

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

CYBER AUXILIARY FOR TACTICAL SOF OPERATIONS

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Mr. Jorge E. Giraldo

AY 2020-21

MMS Mentor Team and Oral Defense Committee Member:
Dr. Brandon Valeriano
Approved: _____
Date: _____

MMS Mentor Team and Oral Defense Committee Member:
Mr. Jeremy Glauber
Approved: _____
Date: _____

Executive Summary

Title: Cyber Auxiliary for Tactical SOF Operations
Author: Mr. Jorge E. Giraldo, United States Special Operations Command

Thesis: Special Operations Forces (SOF) and the Intelligence Community (IC) would benefit from having access to dedicated cyber specialists embedded within the deployed SOF teams to handle extracting, organizing, sorting, and sending the data for timely analysis back to the United States. DoD must adapt to new ways of evaluating talent and be willing to live with non-traditional human capabilities such as not performing physical activities to standard benchmarks. Furthermore, the incorporation of Artificial Intelligence (AI) technologies for triaging and organizing the vast amounts of data collected from the battlefield would benefit SOF and the Intelligence community for producing timely identity intelligence products.

Discussion: SOF operators in theaters of operations are overwhelmed with volumes of captured electronic material. On any given day, approximately four terabytes of data are collected in a single theater of operations. SOF needs the ability to positively identify and attribute an individual's identity to gain knowledge into threat actor planning through collected data at rest. To address the need for expedited data analysis, SOF would benefit from augmenting forensic cyber operators to their deployed locations. However, recruiting, training, and retaining cyber talent for embedding within SOF is easier said than done. The Department of Defense requires changes to its current recruiting techniques to find and attract cyber talent.
Additionally, a reevaluation of how superiors manage the cyber operator's career paths within organizations is required to avoid losing valuable experienced cyber operators to a high-demand market for cyber professionals. Improvements can also be gained by incorporating the latest Artificial technology, which would also accelerate and decrease the vast amount of accumulated data awaiting analysis for intelligence products. This study will provide insights on how cyber auxiliary to SOF can be accomplished.

Conclusion: By implementing a strategy of having forward-deployed cyber operators embedded with SOF to perform DOMEX of collected electronic material and concurrently investing in AI/ML projects that utilize the data collected for teaching the AI algorithms; SOF will continue to provide vital data for actionable intelligence that no other DoD organization can provide. National security threats will reduce by having both AI and cyber forensic operators for support, and in return, it will increase the production of timely intelligence reports.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Table of Contents

Page

EXECUTIVE SUMMARY ii

DISCLAIMER iii

ACKNOWLEDGEMENTS v

Chapter 1 - Introduction 1
Chapter 2 - What Is Cyberspace? 2
Chapter 3 - SOF Currently Engauge In Cyber Tactically In SSE? 4
Chapter 4 - Cyber Workforce Issues 5
Chapter 5 - SOF Cyber Workforce Solutions 9
Chapter 6 - SOF and The Cyber Community 12
Chapter 7 - Unicorn Farms 15
Chapter 8 - Artificial Intelligence and Machine Learning Solutions 18

CONCLUSION 21

CITATIONS AND ENDNOTES 23

BIBLIOGRAPHY 25

Acknowledgments

Throughout my journey in life, I have been blessed to come across a vast amount of influential people that have undoubtedly made a long-lasting impact on my educational experience. Having understood the lesson in life that every day is a learning experience. I am forever grateful to my parents, who taught me a critical lesson. As we get older and focus on accumulating wealth, the most important asset that one can obtain is an education. Further developing your education is a continuous investment to personal success and security. As financial assets may be gained or lost, a solid education cannot be taken away by anyone. With a solid education, one can recover from any challenge that one must confront. For that lesson, I am eternally grateful.

I also would like to express gratitude to my leadership back at USSOCOM. Mr. David Breede, Mrs. Margaret MacCaskey, and Mr. Glen Cullen all encouraged and supported me to apply and succeed at the Marine Corps University to obtain my master's degree. Even while shorthanded at work, they supported my departure to better myself as a professional.

Working and corresponding with Dr. Brandon Valeriano and Lieutenant Colonel Jeremy Glauber has been a privilege. As my mentor for writing this thesis, Dr. Valeriano helped dispel my writing myths and anxieties about technical subjects and showed me how to reach my overall objective in accomplishing this process. As a former Special Forces operator, Lieutenant Colonel Glauber provided subject matter expertise, which reinforced the ideas that I wanted to present.

Writing takes time, patience, and help. I would be remiss if I did not recognize the invaluable and high quality of help from the Leadership Communication Skills Center. If it were not for my writing coaches, Ms. Andrea Hamlen and Ms. Stase Wells, I would not have known how to start

writing a master's thesis and complete the multitude of writing assignments that the Marine Corps University assigns.

My family's support has been essential for me to complete this program. I am very fortunate to have my brother Mauricio continuously checking up on me and giving solid encouragement. Most importantly, my wife and lifelong partner Alessandra, whose continued unconditional love and support during my educational adventure, gave me the solid foundation of emotional support that I needed during stressful times while I was away from home. Thank you for sacrificing your time to take care of Bando while I was gone. Thank you for taking care of our two most beautiful possessions Juliana and Paulina. Additionally, for the everyday sacrifices that you make for all of our benefits.

J. E. Giraldo
Quantico, Virginia
March 2021

Chapter 1 - Introduction

The United States Special Operations Forces (SOF) operators deploy worldwide and perform a multitude of national interest missions daily. For decades, SOF have been recognized as the world's premier counter-terrorism experts with the dominance of the air, land, and sea domains; however, within the cyber domain, SOF is falling behind. While no one domain is less important than others, the cyber domain's limitless boundaries, users, and applications continue to grow at exponential rates. As new threats arise with the proliferation of accessible advanced technology, SOF must have the capability to collect and exploit the valuable data residing within the digital domain in order to quickly analyze and share it with intelligence community (IC) partners to produce actionable intelligence for future operations. United States Special Operations Command (SOCOM) commander General Richard Clarke in the article "SOCOM chief: Door-kickers are out, cyber operators are in" says, "We've been having discussions internally that the most important person on the mission is no longer the operator kicking down the door, but the cyber operator who the team has to actually get to the environment so he or she can work their cyber tools into the fight."[1] SOCOM needs talent that can use and modify software tools to enhance mission objectives, a paradigm that seems to currently be absent. The focus of the cyber operations for SOF, contained within this thesis, relates to the area of digital forensics that is required for Sensitive Site Exploitation (SSE).

Modern technology allows adversaries to maneuver, disseminate data, and hide within global networks with near-total anonymity. When one considers the vast amount of raw data that is being collected from theaters of operation, the US and Department of Defense (DoD) are lagging in the ability to identify and track individual threat actors. SOF needs the ability to positively identify and attribute an individual's identity to gain knowledge into threat actor

planning through collected data at rest. Given the importance of the mission and future missions, SOF and the Intelligence Community (IC) would benefit from having access to dedicated cyber specialists embedded within the deployed SOF teams to handle extracting, organizing, sorting, and sending the data for timely analysis back to the United States. Examinations of current cyber workforce hiring practices within the Department of Defense and commercial industry provide insight into how these organizations might mitigate cyber operator workforce manning shortfalls. Additionally, the United States federal government should consider building cooperative working relationships with the private sector, specifically in the cyber domain. DoD must adapt to new ways of evaluating talent and be willing to live with non-traditional human capabilities such as not being capable of performing physical activities to standard benchmarks. Furthermore, the incorporation of Artificial Intelligence (AI) technologies for triaging and organizing the vast amounts of data collected from the battlefield would benefit SOF and the Intelligence community. Ideally, reducing the workload to SOF operators by incorporating cyber operators and investments in AI technology to help identify valuable data sets to produce critically essential intelligence products is past due. To ensure National security, the Department of Defense must be willing to reinvent military and government civilian positions and concurrently, proactively introduce new technology so that a shift to the risk and consequences from not having threat information are addressed.

Chapter 2 - What is Cyberspace?

According to the DoD Dictionary of Military Terms, cyberspace is "a global domain within the information environment consisting of interdependent networks of information technology infrastructures."[2] Martin Libicki, in “Cyberdeterance and Cyberwar,” says cyberspace is “an agglomeration of individual computing devices that are networked to one

another (e.g., an office local-area network or a corporate wide-area network) and to the outside world."[3] Additionally, Libicki further says cyberspace is composed of three layers: physical, syntactic, and semantic.[4] The physical layer contains hardware that supports data storage, processing, and transportation through cyberspace. The physical layer is ultimately grounded on natural laws (e.g., the speed of light) that govern and limit what is possible. The syntactic layer, in contrast, consists of human-defined protocols and instructions that enable the operation of the physical layer. Finally, the semantic layer represents the information contained in the machine or transmitted across networks.[5] Information and communication technologies have created domestic and global dependence within cyberspace, where economic, social, political, and military interests reside. Every time somebody connects an electronic device to a computer network system, data gets created. According to Nick Galov in "How Many IoT Devices Are There in 2020? [All You Need To Know]," claims that approximately 50 billion devices were connected to the Internet of Things (IoT) in 2020.[6] As data continue to grow, so does the responsibility for SOF to quickly extract, process, exploit, and disseminate data (PED). SOF operators in theaters of operations are overwhelmed with volumes of captured electronic material. On any given day, approximately four terabytes of data are collected in a single theater of operations. Adding to the problem, technical limitations due to bandwidth for transmitting data back to a center for analysis are slow for a large amount of collected information. For example, the transmitting data rates for a 1.2-meter portable satellite deployable node (SDN) are eight Megabits per second (Mbps) up to the orbiting satellite and 16 Mbps down. As a rough estimate, 1 Terabyte of data would take approximately 11.5 days to complete a transmission. Exploitation software is costly and requires operators to have a variety of diverse software program expertise. Because of rapidly evolving consumer trends, Document and Media

Exploitation (DOMEX) toolsets typical in DoD lag behind the commercial sector of electronics and software development.

Chapter 3 - How does SOF Currently Engage in Cyber Tactically in SSE?

The practice of cyber operations for DoD entails three central missions: 1) defend the DoD information networks, 2) defend the US against cyberattacks that produce serious consequences, and 3) support military operations.[7] The focus of the cyber operations for SOF, contained within this thesis, relates to the area of digital forensics that is required for Sensitive Site Exploitation (SSE). SOF SSE is a related series of activities on an objective, collection activity, or sensitive site that allows SOF to identify persons of interest rapidly. The cyber operator's utilization of DOMEX toolsets will enable the establishment of links between those same persons of interest to objects, events, and locations with a high degree of confidence, which will allow for the development of identity intelligence for the collected data.

Today's challenge to SOF and the intelligence community is finding competent coders that can assist with DOMEX software customization for timely digital forensics, providing SOF operators with technical support for timely analysis by intelligence professionals for identity intelligence products. According to US SOCOM commander Army General Richard Clark, SOF in the future will be centered on combating violent extremism; however, SOF will rely heavily on information warfare. General Clarke envisions that SOCOM must prepare itself for "three types of wars: a war on extremism, a war of influence and a war for talent."[8] SOCOM must think about the information space and secure qualified talent to reach dominance in cyber space on a global platform.

Chapter 4 - Cyber Workforce Issue

An unfortunate competition for employment between an attractive commercial sector and the federal government has arisen and led to a significant obstacle for finding experienced people to support SOF. The support that qualified cyber operators would be providing SOF is lured away by salaries that the federal government cannot compete with. Also, elements of personal safety and well-being factor into a cyber operator's employment decision when comparing an excellent luxurious corporate environment to a remote and dangerous forward operating base. In addition, SOF teams are frequently required to deploy to different geographic areas. Finding a cyber operator willing to deploy to a military base outside of the country's comforts will not appeal to many qualified individuals.

Experienced and qualified cyber operators are not easy to find. Unfortunately, for both the Air Force and SOF, no hiring methodology for cyber talent has been created. Authors Michael Sarraille and George Randle in their book, *The Talent War,* do not explicitly address how to find cybersecurity talent but confirm that the DoD's hiring processes need revision. The authors clearly state: "You cannot see talent on the surface; you need a hiring methodology, like basic underwater demolition/ SEAL (BUD/S) training course or the other Special Operations schoolhouses, that reveals it."[9] Application and identification of a straightforward methodology to identify cyber talent must embed support to the ongoing SOF cyber operations.

SOF suffers from the same type of challenges that the RAND Corporation exposed in its study of the Air Force's Cyber workforce. In its February 18, 2018 publication "The Attracting, Recruiting and Retaining Cyberspace Operations Officers," Chaitra Henderson etal. analyzes the shortage of cybersecurity officers within the Air Force. The study draws conclusions from interviews with Air Force Cybersecurity operators at different stages of their careers split into

two distinct officer ranks ranging from (O1-O3) and (O4-O7). The most common reasons for leaving "were low pay and better opportunities in the civilian sector; dissatisfaction with the assignment process; the inability to 'stay on keyboard' or 'remain technical'; and military culture and career field instability."[10] Additionally, the study found that over 75% of the military cyberspace operators believed that they would experience little difficulty finding a job if they left the military.

Factors such as job satisfaction, career progression, knowledge, skills, abilities, and other salient characteristics were analyzed from Air Force personnel offices to recruit and retain talent, leading to vacancies. Furthermore, the long-term impact of economically based program management decisions due to fiscal realities of budget shortages have contributed to talent shortfalls within the cyber workforce. An issue common within the DoD human resources management system is that workforce job descriptions for positions, including cyber positions, are designed as billets associated with set pay grades. Funding for the cyber position is initially calculated by program management when creating a cost estimate for the position's need through a process known as the planning, programming budget, and execution process (PPBE).

The PPBE is a part of the DoD acquisition process, which enables leaders to make decisions to allocate funding for programs and force structures. US defense budget analyst Brendan McGarry illustrates that "DoD policy states that PPBE serves as the annual resource allocation process for the department over a multi-year planning cycle."[11] Cyber operators' salaries and program funding costs are calculated for up to five years and before the year of execution. It is not uncommon to find cost estimates that do not plan for professional retainment and growth. When considering cyber operator career fields, recruiting and retaining challenges will arise if inadequate planning for talent for the required expertise is scarce and not carefully

researched. The lack of fair market value and competitive labor rates for budget calculations and career growth paths will eventually impact programs. For example, let's suppose a new cyber program hires new talent and begins to produce valuable products. Over time, within the program, an employee's gained experience and expertise is now worth and valued more in the commercial world. If the employee desires an increase in pay via a promotion, the employee often is told that they must leave the position and apply elsewhere because the current position was not designed for career growth; it is fixed to a predetermined paygrade. Career growth for exceptional employees is limited to the paygrade associated with the originally designed billets; hence, promotion for high performers to the next step pay grade is often not calculated into the cyber operator's career path, which factors into the employee's desire to continue a career with the organization. Currently, awards such as time off or one-time cash awards are available as retention and motivational tools for management to help maintain a workforce; however, they pale in comparison to promotions. Consider a one-time cash award, while it is nice to receive recognition for good performance, it does not have a long-lasting impact that a small salary increase would have. Consequently, the employee will still be desiring a more competitive salary at the end of the year. Leadership must find a balance to retain exceptional employees with a pay increase versus losing a valuable employee, which seriously impacts a cyber program. Lost momentum, training costs for new employees and reduction in a program's productivity are a few of the issues that management must give proper consideration when creating cyber programs. Proper budget calculations and billet structures that include career growth are vital to avoid the risk of losing a high-performing employee.

In 2020, Sarraille and Randle also provide examples of ineffective hiring practices that organizations routinely commit to, such as failing to identify a person's true character during

their screening process. “One of the biggest issues we’ve identified is that companies don’t know what they’re truly looking for in an employee; instead, they default to making hiring decisions based on past experience and how impressive someone’s resume looks.”[12] They also provide tools for creating acquisition plans for talent identification. Sarraille and Randle describe an experience where a big-name company failed similarly to DoD, “they wanted someone who would fill vacant positions as quickly as possible with people.”[13] DoD’s selection for civilians and military personnel processes adds pressure to hiring managers to fill positions as soon as possible without choosing the best-fit candidates.

The changing nature of warfare and its importance within cyberspace's domain have warranted significant interest concerning US national security. In 2017, Secretary of Defense James Mattis recommended to the President of the United States a change that elevated USCYBERCOM from a sub-unified command status that resided under USSTRATCOM to a Unified Combatant Command. On August 17, 2017, President Donald Trump accepted the recommendation. The US Air Force and its sister services (Army, Navy, Marine Corps) and Air National Guard and Air Force Reserves provided military, civilian, and contractor support to USCYBERCOM as an integral partner of the 133 teams composing the Cyber Mission Force (CMF). The CMF directs, synchronizes, and coordinates all cyberspace operations in defense of US interests. The Air Force experienced workforce challenges with the CMF positions that USCYBERCOM had created. Upon returning from a CMF rotation, a trained and experienced cyber operator did not return to a cyber-related job. Management lost focus on how to properly handle resources. Senator John McCain emphasized this problem in 2017 saying:

> Unfortunately, we have already heard about some puzzling issues. Specifically, out of the 127 Air Force cyber officers that completed their first tour on the Cyber Mission Force, none went back to a cyber-related job. That is unacceptable and suggests a troubling lack of focus. It should be obvious that the development of a

> steady pipeline of new talent and the retention of the ones we have trained already is essential to the success of the Cyber Mission Force.[14]

The Air Force's upper management has frequently mismanaged talent. Cyber operators return to different job duties at the peril of losing valuable warfighting skill sets that are perishable if not continuously practiced. Similarly, Anand Swaminathan and Jürgen Meffert, the authors of *Digital @ Scale*, identify that cyber talent's lack of engagement is due to task saturation within a private corporate environment yields issues with retention and job satisfaction.

Chapter 5 - SOF Cyber Workforce Solutions

In 2014, the IC chief information officer led an effort to transform the IC community's enterprise architecture by developing and establishing standards to facilitate interoperable software language exchange, network configurations, and service protocols. For data to be interoperable, consistent use of extensible markup language (XML) must be applied within data encoding standards to facilitate exchange and maximum interoperability. Collected raw data requires proper labeling. Experience with XML software coding would expedite the processing times required for intelligence purposes. Jack Wiles and Anthony Reyes state in *Best Damn Cybercrime and Digital Forensics Book Period,* "Code writing, scripting, and resource fabrication skills are a welcome addition to the forensic examiner's toolbox!" [15] Experienced forensic cybersecurity specialists who can write code and maintain a top-secret security clearance are scarce. DOMEX tools are developed and sold by specialized companies focused on niche law enforcement entities. Each software program has proprietary code designed without any universal standard for data output. Code writing skills are required to properly customize the software necessary for integration into other platforms.

Implementation of "out of the box" approaches for integrating cyber talent within the SOF community is also required. Serious considerations should be given to allow creature

comforts, changes to dress codes, and physical appearances in order to break free from established military culture. Additionally, passing physical fitness exam requirements serves as a deterrent for wanting to join the military. The DoD could establish alternative direct commissioning programs similar to the Army's direct commissioning pilot program for hiring cyber talent who possess degrees and related certifications that fit recruits for doctors, lawyers, veterinarians, and chaplains. Yasmin Tadjdeh in her article, "Cyber Talent Wanted: Military, Intelligence Community Strive to Retain Cyber Workforces," says, "Officers who join through the initiative are normally awarded three years' worth of credit, allowing them to come in as a first lieutenant and on the precipice of becoming a captain."[16] Furthermore, it is not unusual for doctors to enter the DoD at the rank of colonel. Direct commissioning mechanisms would allow services to acquire highly needed professionals with relaxed physical fitness requirements that non-athletic cyber professionals view as deal-breakers. Cyber talent demand is a certainty, and DoD would benefit by yielding in its physical fitness and a few dress code requirements that will serve as an incentive to talented applicants. Lieutenant General Gina M. Grosso, deputy chief of staff for Manpower, Personnel and Services, US Air Force, states, "How much brawn does the military need, and how much intellect? I think about a cyber warrior. Do I care what a cyber warrior weighs? Do I care if he can run a mile and a half in 12 minutes?"[17] If the overall objective is to build a capable cyber force, then the answer should be no. However, leadership should exercise caution if excluding a service's traditional "rites of passage" such as basic training, as uniformed members may view this as favoritism, which would impede integration and cause tension.

Some cyber operators are motivated by non-monetary remuneration issues. Unsurprisingly, cyber operators are highly motivated by challenges and new technology.

Fielding the latest technology on a yearly cycle to an entire command workforce, including non-cyber operators, is cost prohibitive. At the earliest, program managers typically plan a replacement for information technologies equipment with a three-year capital equipment replacement plan. Having the latest technology sooner than the rest of the force would serve as a motivator to stay satisfied and content with the job at hand. Also, Tadjdeh quotes the Army's cyber training and development director, Sergeant Major Karl Pendergrass says, "We provide them with a unique environment where they get access to things that their counterparts typically do not. They get access to unique mission sets and environments."[18] This notion illustrates that the military and government can provide other areas that commercial tech companies cannot. This paradigm is especially significant when individuals can find challenges that keep their minds interested in solving problems that are not available in the commercial world and add a sense of national pride. The Air Force's chief information officer and director of cyberspace strategy and policy, Major General Patrick C. Higby, echoes the national pride that cyber operators receive when engaged in national interest projects. In his article, "Cyber Talent Wanted: Military, Intelligence Community Strive to Retain Cyber Workforces," he says, "being decisively engaged with an adversary that is trying to do our nation harm — that higher calling will supersede the attractiveness of compensation in the commercial sector."[19] Management must realize that while the government cannot compete with the commercial sector with an operator's financial remuneration, it can provide alternative employee gratification, interest, and uniqueness that brings stability to its cyber workforce.

Chapter 6 - SOF and the Cyber Community

The National Security Agency (NSA) is a member of the IC with a diverse workforce composed of the military, government civilians, and contractor personnel. The NSA and the rest of the IC add a layer to the cyber workforce problem. Every cyber operator within the NSA must obtain a security clearance and be a US citizen. Aside from the time it takes to get a security clearance adjudicated, not having a security clearance limits the pool of competent cyber operators available to the IC. The limited availability of competent operators with a proper security clearance has created a situation where members of the IC compete for talent. Stealing valuable employees from one organization to another is not unheard of due to the high demand for programs to produce intelligence products derived from cyber operators. Program managers from commercial companies who are contracted out for cyber support, have no issues offering attractive salaries to high performing individuals in order to fulfill their company's excellent support requirement to the customer. The IC is diverse with the different capabilities available to those with "a need to know." Unfortunately, stovepipes of information and efforts exist where parallel efforts to solving similar problems are unbeknownst to the government. Resolution to common problems is achieved with better interagency cooperation and communication. Leadership should consider creating programs where employees can rotate among IC agencies to share best practices to insert new blood into programs. By doing so, the government would retain cyber talent and potentially not lose talent to the commercial sector.

DoD defines cybersecurity as "actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication,

confidentiality, and nonrepudiation."[20] USCYBERCOM provides Combatant Commanders with CMF teams to support their missions. Joint Publication 3-12 states,

> Commander, United States Cyber Command (CDRUSCYBERCOM), commands a preponderance of the cyberspace forces that are not retained by the Services. USCYBERCOM accomplishes its missions within three primary lines of operation: secure, operate, and defend the DoD information network; defend the nation from attack in cyberspace, and provide cyberspace support as required to combatant commanders (CCDRs).[21]

Special Operations requires CMF support to be able to extract and process data forensically. Unfortunately, CMF support to SOF was not included in the planning of support for Cyber Operations. USSOCOM, through its joint intelligence directorate (J2), created the Identity Intelligence Operations (I2O) program, and together with the acquisition support from the Program Executive Office Special Reconnaissance (PEO-SR), SOF Operators began training to learn forensic science for the PED of electronic devices found in the battlefield.

In academia, eight cybersecurity career fields are available to pursue: Chief Information Security Officer, Forensic Computer Analyst, Information Security Analyst, Penetration Tester, Security Architect, IT Security Engineer, Security Systems Administrator, IT Security Consultant. Forensic Scientists like detectives analyze computer systems' hard drives and all storage locations to breach data and recover lost data using specialized software. Forensic scientists must employ processes and techniques that ensure data integrity, allowing the use of recovered data for litigation if needed. Of the eight cybersecurity career fields, SOF would benefit most by hiring professionals from the forensic science field. On average, completion of a forensic science bachelor's degree through an accredited university takes four years. Technical forensic science certifications are completed typically in two years. SOF operators learn basic forensic science techniques using the various DOMEX toolsets provided by the Sensitive Site Exploitation program in less than half a year. SOF operators learn the essential concepts of digital forensic

and can perform basic DOMEX activities; however, technical shortfalls in their forensic science abilities are inevitable, suggesting that subject matter experts are required.

SOF operators who have received DOMEX training have deployed to theaters of operations and have successfully collected volumes of data. Approximately 80% of the nation's theater collected data that resides at the National Media and Exploitation Center (NMEC) was collected by SOF. Adding to the problem of having collected vast amounts of data that requires DOMEX, technical limitations with transmitting large data sets back to processing centers for analysis are extremely slow. Could the volumes of data be organized and reduced in size before transmitting back homeland for PED analysis? Would it be possible to send technical support experts to theaters of operations? Employing the XML standards as defined by the Office of National Intelligence's CIO and providing SOF with a computer forensic science analyst with XML programming experience would allow for a more efficient and data processing for analysis of the collected electronic material. The collected raw data requires labeling and triaging down to smaller and relevant data sets before transmission for analysis. These technical forensic specialists have earned the nickname "unicorns" within the SOF community. Successfully finding a unicorn is as hard as keeping a unicorn within an organization, demonstrating why the Identity Intelligence Operations community refers to them as unicorns.

Chapter 7 - Unicorn Farms

SOF, the IC, the commercial industry, and the private sectors all suffer from cyber talent shortfalls. Continued competition for talent amongst all four sectors will not end. However, a strategic change in talent management could be mutually beneficial to all parties if considered. The creation of time-limited exchange programs between all sectors will allow the exchange of problems and solution sets not previously considered by either sector to allow for the cyber talent to gain valuable insights and experience by "getting in other people's shoes." SOF could leverage the commercial sector's cybersecurity forensic scientists' expertise by deploying with an individual to a safe location where sensitive site exploitation occurs. The mutual benefits that such relationships will produce are two-fold: 1) The commercial industry will gain detailed information on how SOF uses their DOMEX tools and the shortfalls of the products for enabling SOF (and the IC) to identify and track threat actors, and 2) the Cyber forensic scientists who understand the software product's coding could then access and modify the program's internal algorithms to produce the desired data products for SOF to submit to the IC. Furthermore, the commercial industry is continuously looking for experiences from their customers for product improvements and new areas for product development. By deploying with SOF, they would be acquiring the knowledge needed for growth. For SOF, the benefit from the commercial sector's cybersecurity forensic scientists' presence is significant in two ways. The first benefit will be from the reduction of data from theater collected hard drives. The collected hard drives are triaged and downsized into data sets for categorization while irrelevant data is discarded. The new smaller data sets of interest are then sent to intelligence analysts for intelligence production, thus saving transmission times back to the United States from locations without reliable bandwidth. With SOF providing organized and triaged data sets to the IC for intelligence

products, future threat actors can be identified and tracked removing opportunity for bad actors to inflict damage. Secondly, SOF will be able to get intelligence products back from the IC sooner, in a shorter time, while reducing the risk of missing a window of opportunity to find, fix, and finish national threats.

Curiously, if the civilian who gained experience while undergoing a rotation with a SOF element were to desire to join the military, a change to the enlistment process is required. In his article “The Pentagon’s controversial plan to hire military leaders off the street," Andrew Tilghman provides an example that highlights the necessary changes required for enlistment into military service. Tilghman hypothetically proposes if Mark Zuckerberg, whose “skills would likely be profoundly valuable to US Cyber Command, the 32-year-old computer programmer dropped out of Harvard and has no bachelor's degree, making him ineligible for commission as an officer. A military recruiter could probably find some ways to grant him credit for the skills and experience evident in his self-made fortune — estimated to be $51 billion — but not much.”[22] Mark Zuckerberg would probably make the grade of E-4 at Cyber Command.[23] The military should have the ability to bring a person with high a caliber of talent into ranks best suited for leadership roles. By doing so, the new military allocates the new cyber operator member the authority to make changes for improving CYBERCOM systems if deemed necessary.

Protecting classified information causes questions to arise from security managers regarding the nature of SSE collection and exploitation of data. All the data collected from sensitive site exploitation activities within theaters of operation is considered unclassified. The requirement for the cyber operator to have a security clearance is not necessary to perform digital forensics. Nevertheless, possession of a security clearance is beneficial from the operational

security perspective. If the nature of certain specific missions is classified, it is a good idea for operations security purposes to surround personnel with security clearances adjudicated around SOF operations. The IC partners have cyber operators who possess security clearances. As part of a managerial development and retainment program amongst IC members, a rotation of cyber operators who can assist with SOF in theaters of operations. A time-limited memorandum of understanding signed by senior leadership for the rotational support for SOF will allow the cyber operator to deploy with SOF teams. SOF will benefit from the cyber operator's expertise to streamline data sets. Concurrently, the cyber operator will develop first-hand experience gained by working with and customizing the DOMEX software (if necessary) to produce valuable data sets for intelligence products. The type of experience gained by the cyber operator is unique and rewarding because the fruits of hard work will not be unnoticed. Additionally, the Department of Defense will have produced something that it is in a deficit of possessing, a unicorn.

As much as SOF and the IC would benefit from unicorns, producing a large workforce with specialized forensic cyber talent will not be easy. Atomization by computers "that mimic human intelligence through behaviors which are typically associated with cognitive functions such as learning and problem solving."[24] Artificial intelligence is an area that shows promise to help lighten the forensic science workloads placed on cyber operators, intelligence analysts, and the warfighter. Currently, artificial intelligence can accomplish particular tasks in limited environments. However, it is a technology that is at a maturity level worth consideration for DOMEX applications.

Chapter 8 - Artificial Intelligence and Machine Learning Solutions

Today, Artificial Intelligence (AI) and Machine Learning (ML) technology has positioned itself as the most promising application to address the processing of the vast amounts of data that undergoes DOMEX[25]. By autonomously sorting and identifying data files by types from keywords or image searches, AI/ML algorithms will provide intelligence officers timely data sets for forensic analysis, which will minimize threats to national security.

Multiple petabytes of backlogged collected digital data reside at the NMEC. Funding shortages that provide resources for forensic analysis have hindered timely intelligence products. *Research Digest's* Matthew Warren states the average reading rate is 238 words per minute.[26] On average, students can read a page of single-spaced 12-point New Times Roman font in two minutes. In her article “How many words per page?” Kari Lisa Johnson says that 500 words for single spacing constitute a single page.[27] A terabyte of digital storage capacity can store 75 million pages. Electronic discovery automation company Cloudnine calculates for one terabyte of data, "it would take more than 185 reviewers working 2,000 hours each per year to complete the review within a year."[28] When the interest for timely intelligence reporting is essential, the insertion of AI/ML technology can significantly lower unachievable workloads by sifting through the volumes of data, removing irrelevant data, and potentially highlighting data sets for intelligence analysts.

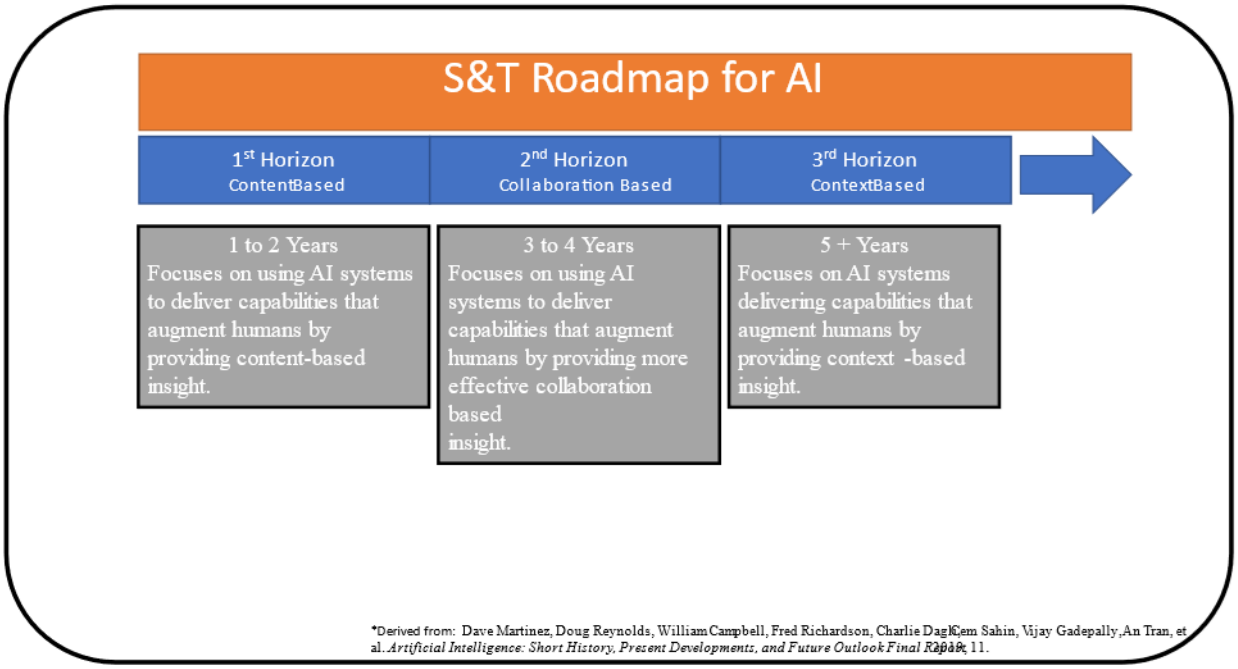
Data conditioning is critical for the effectiveness of which AI/ML performs. Machine learning algorithms require data conditioning for data that resides within its neural networks. AI requires that the data type needs to be tabular, imagery, or text. Dr. Julia Mullen from MIT Lincoln Laboratories states, "we need to identify the proper type and appropriate volume of raw data required for the learning algorithm."[29] Furthermore, according to *Artificial Intelligence:*

Short History, Present Developments, and Future Outlook, "Data conditioning can account for nearly 80% of the time consumed in developing AI applications."[30] Hiring intelligence analysts with the sole task of identifying and producing reliable, clean data sets for use in either supervised or unsupervised machine learning should be a priority investment from SOF and the IC.

AI is vulnerable to data poisoning and spoofing. Having intelligence analysts provide clean data sets is vital for developing the AI models required for producing reliable algorithms. The vast majority of collected hard drives and electronic material arrive from unsophisticated sources, representing a roadblock to correctly identifying data sets and introduces the risk of assimilating poisoned data. “However, human involvement can provide ground truth to data sets and mitigate the risk of incorporating poisoned data sets into the learning models.”[31] National vulnerability databases were created to serve as a protection mechanism for preventing spoofed data injection into new learning models. The databases use updated data to ensure that clean data is analyzed before ingesting poisoned data into learning AI algorithms[32]. Like antivirus software, continuous updating of the anti-spoofing technology used for protecting learning algorithms is unavoidable for AI models to mature.

Dr. Dave Martinez from MIT Lincoln Labs is an AI expert who presents a roadmap of three Science and Technology (S&T) investment horizons where AI capabilities can be operational within a five-year time frame. Content-based insight is the first horizon that is achievable in one to two years. Reduced user workload, improved confidence in AI, and robust AI are attainable are the benefits that are within reach of this first horizon. Collaboration-based insight, the second horizon, is where human-machine teams work together to outperform an expert in challenging cognitive tasks. Dr. Martinez states that “this horizon requires that we

extend AI roles to include multiple human-machine teams working together."[33] He adds that when machines aid humans, their collaborative output outperforms experts when performing complex cognitive tasks. He claimes that "humans are much better than a machine at making subjective judgments, disambiguating options, and understanding context."[34] Investing today in this collaboration-based horizon is achievable within three to four years. Finally, the last horizon, context-based insight, is an area that requires the most development. It will take at least five years to develop. It is "where machines can provide recommendations with a high degree of confidence by incorporating relevant knowledge from other related inputs"[35] in reduced time. SOF and the IC do not need to reach the third horizon for AI to begin to provide an output that intelligence officers can appreciate. Incorporating AI data produced from within the first horizon will immediately help reduce extremely high workloads. The S&T roadmap for AI may also be visualized with the following chart:



*Derived from: Dave Martinez, Doug Reynolds, William Campbell, Fred Richardson, Charlie Dagli, Cem Sahin, Vijay Gadepally, An Tran, et al. *Artificial Intelligence: Short History, Present Developments, and Future Outlook Final Report*, 2018, 11.

The incorporation of AI technology for analyzing the data from collected electronic material has multiple benefits. Removing the workloads and saving time using AI to downsize data sets for intelligence analysts and SOF cyber support is a welcoming scenario that could begin at the first horizon. “SOF is amenable to working with the proposed AI technology for data forensics at a 70% maturity level. Productive and timely intelligence reports will provide theater commanders sufficient information that will allow SOF missions to find enemy combatants quicker”[36]. Expeditiously finding bad actors will justify funding for development, sustainment and will enhance national security.

Conclusion

Data storage capacity continues to grow while transistor fabrication still follows Moore’s law. The commercial world now has various available models of smartphones, which each can store up to 1 Terabyte of data. To put that capacity into perspective, up to 1000 high-definition movies can be stored on a single phone with room to spare. As DoD focus shifts to near-peer threats, adversaries undoubtedly will have the ability to produce and hide significantly more data than is being analyzed today.

Talent shortfalls for Cybersecurity operators exist and will continue to grow. SOF and the Intelligence Community would benefit from having access to dedicated cyber specialists embedded within the deployed SOF teams to handle extracting, organizing, sorting, and sending the data for timely analysis back to the United States. Embedding forensic science trained cyber operators with SOF at the front end inside theaters of operation until Artificial Intelligence or Machine Learning (AI/ML) technology is mature enough to be gradually incorporated in the forensic processes would aid the identity intelligence process.

Backlogs of unanalyzed data accumulate, making operators question why they should even risk themselves if the data will reside at a government location unanalyzed. Leaders recognize that good data feeds intelligence reports, which in turn helps decision-making. As advancements in chipsets required for AI evolve, so does AI's opportunity to produce data sets that intelligence analysts require to produce and share opportune reports. With increased valuable intelligence reporting output derived from AI, mission success increases, and AI's investment will also increase. SOF and IC investments are required immediately for reaching the third AI/ML horizon level of capability within five years. The NMEC's backlogs for forensic data analysis for intelligence reports will decline once AI has good, conditioned data for learning algorithms. National security will improve even if the AI models start providing data sets that are not at 80 to 100% confidence intervals. AI will provide intelligence officers and the overall IC, much-needed help for producing timely intelligence reports and thus reduce national security threats.

By having forward-deployed cyber operators embedded with SOF to perform DOMEX of collected electronic material and concurrently investing in AI/ML projects that utilize the data collected for teaching the AI algorithms, SOF will continue to provide vital data for actionable intelligence that no other DoD organization can provide. Why? Because no one else is at the front end of the battlefield collecting the electronic material, which provides the raw data for identity intelligence required to find the actors and the organizations that threaten the nation. SOF does not have a lack of data problem. SOF has an overwhelming amount of collected data that contains information that would benefit both SOF and the IC if it incorporates expert forensic cyber operators and artificial intelligence to lighten the ever-growing backlogs and workloads.

Citations and End Notes

[1] Jared Keller, "SOCOM chief: Door-kickers are out, cyber operators are in," *Task & Purpose* (May 2020), 2, https://taskandpurpose.com/news/special-operations-forces-cyber-warfare/
[2] Joint Chiefs of Staff. *DOD Dictionary of Military and Associated Terms*, Instruction 5705.01F, June 2020, 55, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.
[3] Martin Libicki, *Cyberdeterence and Cyberwar,* RAND Corporation Project Air Force PAF, (Santa Monica, CA: RAND Corporation, 2009), 6, https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf
[4] Martin Libicki, *Cyberdeterence and Cyberwar,* RAND Corporation Project Air Force PAF, (Santa Monica, CA: RAND Corporation, 2009), https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf
[5] Martin Libicki, *Cyberdeterence and Cyberwar,* RAND Corporation Project Air Force PAF, (Santa Monica, CA: RAND Corporation, 2009), https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf
[6] Nicholas, Galov "How Many IoT Devices Are There in 2020? [All You Need To Know]", accessed November 11, 2020, https://techjury.net/blog/how-many-iot-devices-are-there/#gref
[7] Government Accountability Office. *DOD TRAINING U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force* (Washington, DC: Government Accountability Office, 2019), 2, https://www.gao.gov/assets/700/697268.pdf .
[8] Jared Keller, "SOCOM chief: Door-kickers are out, cyber operators are in," *Task & Purpose* (May 2020), 2, https://taskandpurpose.com/news/special-operations-forces-cyber-warfare/
[9] Sarraille, Mike. The Talent War: How Special Operations and Great Organizations Win on Talent (p. 33). Lioncrest Publishing. Kindle Edition.
[10] Chaitra Henderson, M., Leslie A. Payne, John A. Hamm, Angela Clague, Jaqueline Torres, David Schulker, and John S. Crown. *Attracting, Recruiting, and Retaining Successful Cyberspace Operations Officers*, RAND Corporation Project Air Force PAF, (Santa Monica, CA: RAND Corporation, February 12, 2018), 48, https://www.rand.org/pubs/research_reports/RR2618.html
[11] Brendan W. McGarry, *Defense Primer: Planning, Programming, Budgeting and Execution (PPBE) Process*, CRS Report for Congress IF10429 Version 9 (Washington, DC: Congressional Research Service, December 11, 2020), 1, https://fas.org/sgp/crs/natsec/IF10429.pdf.
[12]Sarraille, Mike. The Talent War: How Special Operations and Great Organizations Win on Talent (p. 24). Lioncrest Publishing. Kindle Edition
[13] Sarraille, Mike. The Talent War: How Special Operations and Great Organizations Win on Talent (p. 41). Lioncrest Publishing. Kindle Edition
[14] Chaitra Henderson, M., Leslie A. Payne, John A. Hamm, Angela Clague, Jaqueline Torres, David Schulker, and John S. Crown. *Attracting, Recruiting, and Retaining Successful Cyberspace Operations Officers*, RAND Corporation Project Air Force PAF, (Santa Monica, CA: RAND Corporation, February 12, 2018), 86, https://www.rand.org/pubs/research_reports/RR2618.html.
[15] Wiles, Jack, and Anthony Reyes. The Best Damn Cybercrime and Digital Forensics Book Period : Your Guide to Digital Information Seizure, Incident Response, and Computer Forensics, Elsevier Science & Technology Books, 2007. 50
[16] Yasmin Tadjdeh, "Cyber Talent Wanted: Military, Intelligence Community Strive to Retain Cyber Workforces," *National Defense Magazine* NDIA's Business and Technology Magazine (2018), 28, https://www.nationaldefensemagazine.org/articles/2018/2/26/cyber-talent-wanted-military-intelligence-community-strive-to-retain-cyber-workforces.
[17] Unknown, "Air Force Finally Coming around on Fitness." John Q. Public (blog), October 13, 2016, https://jqpublicblog.com/air-force-finally-coming-around-fitness/
[18] Yasmin Tadjdeh, "Cyber Talent Wanted: Military, Intelligence Community Strive to Retain Cyber Workforces," *National Defense Magazine* NDIA's Business and Technology Magazine (2018), 28, https://www.nationaldefensemagazine.org/articles/2018/2/26/cyber-talent-wanted-military-intelligence-community-strive-to-retain-cyber-workforces.

[19] Maj. Gen. David Higby, quoted in Yasmin Tadjdeh, "Cyber Talent Wanted: Military, Intelligence Community Strive to Retain Cyber Workforces*," National Defense Magazine* NDIA's Business and Technology Magazine (2018), 28, https://www.nationaldefensemagazine.org/articles/2018/2/26/cyber-talent-wanted-military-intelligence-community-strive-to-retain-cyber-workforces.
[20] US Department of Defense *DOD Dictionary of Military and Associated Terms,* Joint Publication 1, June 1, 2020, 56.
[21] US Joint Chiefs of Staff, *Cyberspace Operations,* Joint Publication 3-12 (Washington, DC: Joint Chiefs of Staff, June 8, 2018), I-8.
[22] Andrew Tilghman, "The Pentagon's Controversial Plan to Hire Military Leaders Off the Street," *Military Times*, 19 June 2016, 6, https://www.militarytimes.com/2016/06/19/the-pentagon-s-controversial-plan-to-hire-military-leaders-off-the-street/
[23]Ibid
[24] Shah, Danelle, "Introduction to Machine Learning," Lecture 1, MITLL: MITLLx220 Survey of Artificial Intelligence and Machine Learning, accessed February 21, 2021, 1:37, https://llx.mit.edu/courses/course-v1:MITLL+MITLLx220+Winter_2021/courseware/efb68778d4b64eaab6ee3f2ced32cde7/25103f3256ed40679b46ad38fb0c110d/
[25] Jorge E. Giraldo, "Survey of Artificial Intelligence and Machine Learning" (unpublished manuscript, February 5, 2021), Microsoft Word file.
[26] Warren, Matthew, "Most Comprehensive Review To Date Finds The Average Person's Reading Speed Is Slower Than Previously Thought," Research Digest, June 13,2019, https://digest.bps.org.uk/2019/06/13/most-comprehensive-review-to-date-suggests-the-average-persons-reading-speed-is-slower-than-commonly-thought/.
[27] Kari Lisa Johnson, "How amny words per page?," The Word Counter, October 18, 2019, accessed March 3, 2021, https://thewordcounter.com/how-many-words-per-page.
[28] Comments, No, "eDiscovery Best Practices: Perspective on the Amount of Data Contained in 1 Gigabyte," Cloudnine, accessed February 5, 2021, https://cloudnine.com/ediscoverydaily/electronic-discovery/ediscovery-best-practices-perspective-on-the-amount-of-data-contained-in-1-gigabyte/#eut-comments
[29] Mullen, Julia, "Introduction to Data Requirements and Conditioning," Lecture 2, MITLL: MITLLx220 Survey of Artificial Intelligence and Machine Learning, accessed February 5, 2021, 5:56, https://llx.mit.edu/courses/course-v1:MITLL+MITLLx220+Winter_2021/courseware/efb68778d4b64eaab6ee3f2ced32cde7/25103f3256ed40679b46ad38fb0c110d/
[30] Dave Martinez, Doug Reynolds, William Campbell, Fred Richardson, Charlie Dagli, Cem Sahin, Vijay Gadepally, An Tran, et al. *Artificial Intelligence: Short History, Present Developments, and Future Outlook Final Report* 2019, 38.
[31] Jorge E. Giraldo, "Survey of Artificial Intelligence and Machine Learning" (unpublished manuscript, February 5, 2021), Microsoft Word file.
[32] Jorge E. Giraldo, "Survey of Artificial Intelligence and Machine Learning" (unpublished manuscript, February 5, 2021), Microsoft Word file.
[33] Dave Martinez, Doug Reynolds, William Campbell, Fred Richardson, Charlie Dagli, Cem Sahin, Vijay Gadepally, An Tran, et al. *Artificial Intelligence: Short History, Present Developments, and Future Outlook Final Report* 2019, 117.
[34] Dave Martinez, Doug Reynolds, William Campbell, Fred Richardson, Charlie Dagli, Cem Sahin, Vijay Gadepally, An Tran, et al. *Artificial Intelligence: Short History, Present Developments, and Future Outlook Final Report* 2019, 117.
[35] Dave Martinez, Doug Reynolds, William Campbell, Fred Richardson, Charlie Dagli, Cem Sahin, Vijay Gadepally, An Tran, et al. *Artificial Intelligence: Short History, Present Developments, and Future Outlook Final Report* 2019, 117.
[36] Jorge E. Giraldo, "Survey of Artificial Intelligence and Machine Learning" (unpublished manuscript, February 5, 2021), Microsoft Word file.

Bibliography

_____. Joint Publication 3-12, *Cyberspace Operations*. Washington, DC: Department of Defense, 2013. *DoD Cyberspace Workforce Strategy signed (Final)* 2013.

Frost, Wendy. "University of Texas at San Antonio; UTSA Gets $2 Million to Train National Security Analytics Cyber Workforce." *Defense & Aerospace Week,* October 2018. https://www.utsa.edu/today/2018/10/story/DIA-MSDAprogram.html.

Hardison, Chaitra M., Leslie Adrienne Payne, John A. Hamm, Angela Clague, Jacqueline Torres, David Schulker, and John S. Crown, *Attracting, Recruiting, and Retaining Successful Cyberspace Operations Officers: Cyber Workforce Interview Findings*. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR2618.html.

Hess, William W. and Robert M. Moore. "Defensive Cyberspace Operations." *Marine Corps Gazette* 102, no. 4 (2018): 44-48. https://search-proquest-com.lomc.idm.oclc.org/docview/2026328619?accountid=14746.

Liang, John. "Pentagon Bid for Cyber-Specific Workforce Rejected by Lawmakers." *Inside Cybersecurity* (2019). https://search-proquest-com.lomc.idm.oclc.org/docview/2268987781?accountid=14746.

Machi, Vivienne. *Special Operations Forces Intel Units Need Help Wading through a Flood of Data* 2017.

McMahon, Christopher J. and Colin J. Bernard. "STORM CLOUDS ON THE HORIZON: Challenges and Recommendations for Military Recruiting and Retention." *Naval War College Review* 72, no. 3 (2019): 84-100. https://search-proquest-com.lomc.idm.oclc.org/docview/2246150612?accountid=14746.

Nelson, Janel. "Beefing Up the Cyber Workforce." *Signal* 73, no. 9 (2019): 37-39. https://search-proquest-com.lomc.idm.oclc.org/docview/2226332229?accountid=14746.

Nuño, Geronimo. *Chateau Cyber: Applying Historical Events to Military Innovation in the Cyber Domain*. Reading, United Kingdom Reading, Reading: Academic Conferences International Limited, 2018. https://search-proquest-com.lomc.idm.oclc.org/docview/2018924801?accountid=14746.

Pătrașcu, Petrișor. "Missions and Actions Specific to Cyberspace Operations." *International Conference KBO* 25, no. 3 (Jun 01, 2019): 51-56. doi:10.2478/kbo-2019-0117. http://www.degruyter.com/doi/10.2478/kbo-2019-0117.

Payne, John A. Hamm, Angela Clague, Jaqueline Torres, David Schulker, and John S. Crown. *Attracting, Recruiting, and Retaining Successful Cyberspace Operations Officers*. Santa Monica, CA: RAND, 2019. https://www.rand.org/pubs/research_reports/RR2618.html

Ramsey, Aric A. "Talent Management for Cyber Warfare." *Marine Corps Gazette* 104, no. 4 (2020): 56-59. https://search-proquest-com.lomc.idm.oclc.org/docview/2391979440?accountid=14746.

Reynolds, Doug, William Campbell, Fred Richardson, Charlie Dagli, Cem Sahin, Vijay Gadepally, An Tran, et al. *Artificial Intelligence: Short History, Present Developments, and Future Outlook Final Report* 2019.

Rogers, Michael. "A Challenge for the Military Cyber Workforce." *Military Cyber Affairs* 1, no. 1 (Dec, 2015). doi:10.5038/2378-0789.1.1.1012.

Seffers, George I. "Calling for a Civilian Cyber Corps." *Signal* 73, no. 9 (2019): 41-43. https://search-proquest-com.lomc.idm.oclc.org/docview/2226332239?accountid=14746.

Shattuck, Jeremy A. "Defense Industry must Learn to Woo Millennials." *National Defense* 104, no. 797 (2020): 16-17. https://search-proquest-com.lomc.idm.oclc.org/docview/2403117038?accountid=14746.

Tadjdeh, Yasmin. "Cyber Talent Wanted." *National Defense* 102, no. 772 (2018): 26-29. https://search-proquest-com.lomc.idm.oclc.org/docview/2031701106?accountid=14746.

Towers Watson, Wilson. "Most Global Organizations Fail to Learn from Cyber Mistakes: WTW Survey." *Insurance Journal,* June 2018. https://www.insurancejournal.com/news/international/2018/06/22/493087.htm

US Department of Defense. Cyberspace Workforce Management, Directive 8140.01, October 5, 2020. Accessed February 15, 2021. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001p.pdf?ver=2019-06-06-120639-863

US Government Accountability Office. DOD TRAINING: US Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force. GAO-19-362. Washington. DC, 2019. Accessed February 16, 2021. https://www.gao.gov/assets/gao-19-362.pdf.

US Government Accountability Office. HUMAN CAPITAL: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government. GAO-04-546G. Washington. DC, 2019. Accessed November 16, 2020. https://www.gao.gov/products/gao-04-546g

US Office of the Director of National Intelligence. Intelligence Community Technical Specification XML Data Encoding Specification for Document and Media Exploitation Version 2. May 09, 2014.