A CYBER RESERVE FUTURE

Capturing Loss, Re-Imagining Utilization, and an Introduction to Geographic Alignment

MAJOR ZEV MCCARTY
ADVISOR: DR. JOSHUA SIPPER
AIR UNIVERSITY: AIR COMMAND STAFF COLLEGE

22 MARCH 2024

"The conclusions and opinions expressed in this research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, Department of Defense, or The Air University."

In the face of rapidly evolving cyber threats and the increasing sophistication of adversaries, the United States Cyber Forces face a critical challenge: an acute shortage of cyber specialists. To effectively address this challenge and enhance the effectiveness of its cyber reserve component, the Department of Defense (DOD) should adopt a hub-and-spoke model centered at Naval Air Station-Joint Reserve Base Fort Worth. This strategic approach would capitalize on the geographic concentration of cyber talent, facilitate collaboration with local industry partners, and foster a deeper integration of civilian and military expertise, ultimately strengthening the DOD's ability to defend against cyber threats and protect its critical infrastructure and networks.

Defining the Cyber Force

First, we must define the cyber force within the United States. In the United States, the cyber force consists of private and government sectors. The latter comprises multiple defense and civilian agencies, departments, services, and organizations—for example, the National Security Agency, Central Intelligence Agency, and Federal Bureau of Investigations. The former consists of every person, business, or entity (NGO, for example). For the sake of this review, the prominent players in the cyber and tech private sector will be the basis of discussion. This review compares, contrasts, and relates these prominent players to the DOD military branches. For further clarity in the discussion, "cyber forces" will be defined as "…a kind of military organization with some degree of authority over cyber operations."[1]

These DOD forces employ cyber operations offensively and defensively to deny, disrupt, delay, degrade, or destroy enemy forces, including opposing personnel. Cyber forces historically were utilized as enablers to forces of conventional domains (air, land, and sea) and their kinetic operations; however, in recent decades, this has expanded. Though the government and private sectors differ in scale or focus of operations, the schemes and disciplines are vastly different.

The private sector defines the cyber field as Information Technology (IT) and Information Security (INFOSEC). The DOD differs and categorizes cyber into operations or "cyberspace operations" which are Offensive Cyber Operations (OCO), Defensive Cyber Operations (DCO), and Department of Defense Information Network (DODIN).[2] IT, an industry term, is defined, in a RAND study on lessons learned, as a "…tasks related to providing cyber services, including operation and maintenance of computer systems, networks and data; requirements planning; knowledge management and in-house software and systems development; computer user and network support; and software assurance."[3] Experts in IT have transferrable skills across various cyber operational mission sets, most specifically handling the physical layers of cyber, IT, and infrastructure to "…provide storage, transport, and processing of information within cyberspace…" while the passwords or "..IT user accounts" are utilized to develop the cyber-persona layer of actors or entities.[4] Differing, INFOSEC is closer to the DOD cyber specialty of active and passive defensive cyber operations (DCO), consisting of tasks related to "…protecting and defending systems and networks; detecting, investigating, and responding to security incidents; ensuring information assurance compliance; performing security systems development and designing system security architectures." [5] This is not to say that there are no overlaps or parallels between various aspects of civilian and military practices, only that they are distinct in definitions and roles in the two separate sectors.

Of these two sectors, the private sector workforce consists of approximately 95% IT personnel. [6] Furthermore, the private sector can also retain these personnel for a long time, thus allowing the private sector and its personnel opportunities to build extensive IT technical expertise that the DOD cannot. [7] Nevertheless, the emphasis on IT has led the private sector to outsource INFOSEC or depend on alternative methods, such as government entities, to safeguard their interests. In contrast to the private sector, the DOD must prioritize INFOSEC, particularly Defensive Cyber Operations, due to the nature of adversaries, ongoing attacks in both peacetime and wartime and the vital importance of protecting DOD weapon systems and critical infrastructure.

The INFOSEC discipline highly demands the DCO's cyber skills and career specialty. However, OCO and DODIN personnel face a higher risk of retention problems than the smaller than 5% of the workforce that benefits from translating skills in the DCO specialty. [8] This results in our overall DOD force needing more depth of experience in the OCO and DODIN roles rather than in the DCO role. In this situation, the Reserve component plays a crucial role as a key enabler. We must build a force to capture former, experienced officers and NCOs. Also, we must access talented and experienced individuals from the private sector, leveraging civilian-military strengths (technology, relationships, etc.) to meet DOD needs. Best leveraged as a mechanism for capturing existing experience rather than developing talent, the Reserves offer an avenue for retaining expertise. This recapturing of talent is important because current retention rates for cyber specialists stand at a mere 9%, presenting a significant challenge.[9] The Reserve component offers a solution to recapture the loss of these experienced personnel.

Alignment, Geography, and Civ-Mil Posturing: Hub Spoke Model

The DOD leadership must adopt, a hub-and-spoke model (Figure 1) centered at Naval Air Station Joint Reserve Base Fort Worth to aid recruitment and retention. Cyber-reserve components aim to harness the geographic position and economic trends of the United States' cyber and tech workforce. The American workforce consists of approximately 5.5 million people specializing in tech. Over 400,000 reside within the Texas triangle (Austin, Dallas–Fort Worth, Houston, and San Antonio), more than any other region in the United States. Austin has the fifth-largest concentration of software engineers, with 59.2% of the IT professionals being software engineers. [10] Furthermore, all four major Texas cities have seen substantial growth in crucial education fields of Computer Engineering, Math/Statistics, and Other Tech Engineering. With San Antonio increasing by 39% between 2016 and 2020, then Austin (+23%), Dallas-Ft Worth (+21%) and Houston (+15%) during the same period. [11] Texas is a center-of-gravity for the tech industry, which is also conveniently home to multiple military installations and geographically central within the United States.

Integrating a reserve component for cyber must consider first geography and second utility. Geographically, the challenge lies in the presence of military bases and civilian career centers. To strategically address this constraint, a hub is established, strategically centered around Naval Air Station-Joint Reserve Base Fort Worth. Positioned at the geographical center of the country, this base strategically provides convenient access, both by driving and flying, to major cities in the field of cyber. Moreover, it strategically aligns with two major civilian aviation hubs: Dallas Fort-Worth and Dallas Love Field--placing such cities as Austin, San Antonio, San Francisco, Dallas, DC Metro, and Fort Eisenhower by extension of Atlanta in reach of the Joint Base. In addition to Naval Air Station-Joint Reserve Base Fort Worth, Fort Worth is home to the United States Air Force Reserve's 10th Air Force, responsible which for 17 operational units including bomber, fighter, cyber, and intelligence units, most of which are within close-proximity. Furthermore, Fort Worth is within commutable distance to multiple cyber-focused units: 16th Air Force (AFCYBER), 33rd Cyber Operations Squadron (COS), and 616th Ops Center at Lackland AFB, TX, near San Antonio, as well as the major army installation of Fort Cavazos. Positioning at Joint Reserve Base Fort Worth will place the reserve component in the center of civilian and military operations, allowing access to a larger recruiting pool while supporting an extensive portfolio of units.

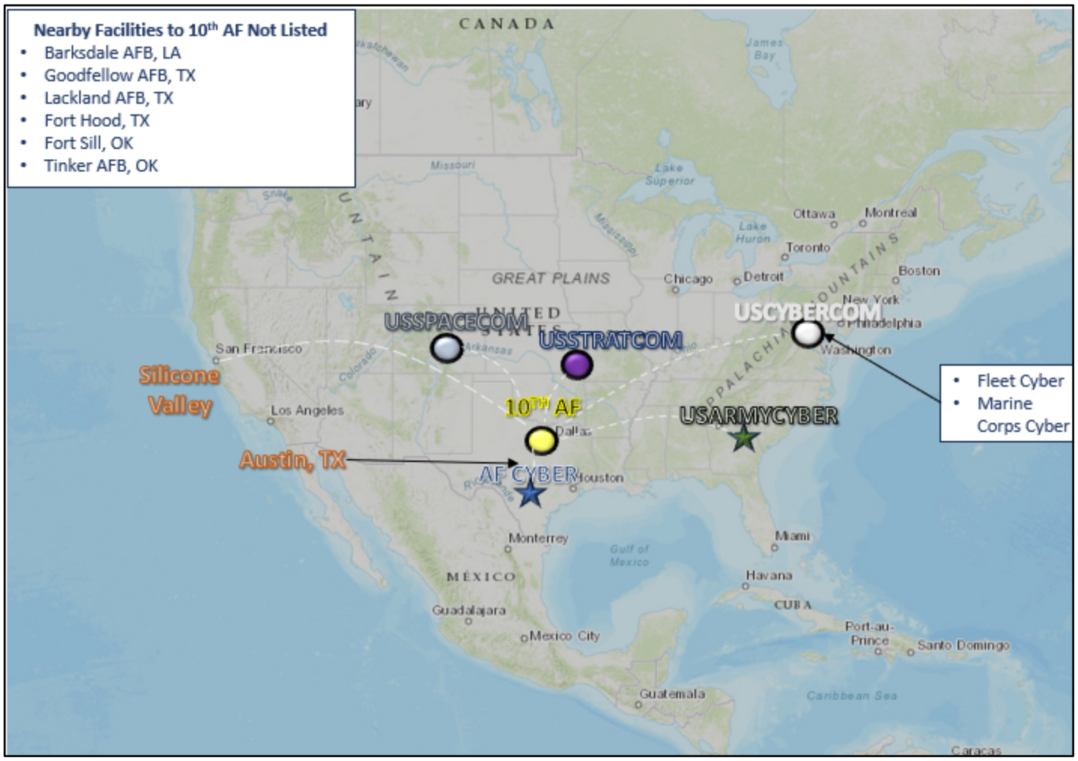

Fig. 1: Concept of Geographic Cyber Alignment

The Correct amount of Experience and Tenacity, the Reserve Force

The Structure, Strengths, and Gaps

One must understand that the Reserve component is not an active component or managed similarly. The Reserve component consists of multiple personnel manning positions that relate to a term called statuses. Reserve component statuses and positions include four categories:

Individual Mobilization Augmentee (IMA), Active Guard Reserve (AGR), Traditional Reserve (TR), and Reserve Technicians. AGR and ART personnel serve similarly to Active-Duty personnel and typically maintain continuity within units, often filling key leadership positions. Though AGR and ART personnel are crucial to a reserve unit's function, the role of cyber and its unique talent needs, require a balance toward utilizing more IMA and TR category members.

The IMA is a "…trained, equipped, and ready reservist when the service needs them to support an operational requirement." [12]This reservist is typically someone with prior experience and works at an operational or higher level, augmenting active-duty units.[13] Think of an Airman filling an Air Operations Center (AOC) role or a soldier at the Division staff who fills a deployed or supporting function when needed. Often, these are FGO and NCO-level positions. Mobilization periods can vary in length, typically 24 flexible schedule days and 14 annual training days, depending on the needs of the unit. However, this is often a few weeks a year in peacetime. However, not every IMA position is the same; some require more commitment than others. The objective of the IMA program is to have augments that can immediately augment active-duty units in times of war or national crisis—accomplished through training prior to such events. These augments reduce the lag time associated with bringing in outside personnel and acquainting them with the personalities and relationships of such units. Therefore, an experienced IMA can provide seamless and immediate support to a unit. [14] Traditional Reservists, in contrast, serve two weeks annually and two drill periods, as a minimum, and are best utilized at the operational or tactical level. They are flexible and maintain currencies and qualifications to remain capable to employ. Such currencies can be deployment-related, such as M9 training and CBRNE, or specialty-specific, such as nuclear weapons delivery or night landings. Each specialty and unit, including cyber, requires differing currencies and qualifications. TRs currently make up most of the reserve component, performing approximately 20 percent of the daily missions for the Air Force and, for Aeromedical, up to 65 percent of the missions. [15]

Employing for Effect

How will we employ Cyber IMA officers and enlisted? These individuals, with prior experience, are crucial, and instead of losing their experience, the IMA allows us to retain them. IMA's best fit the needs of higher headquarters, such as 10th AF, and should be aligned explicitly with a supported unit. An Air Force example of this would be an IMA to Air Force Global Strike Command. The Cyber IMA should spend his/her training days in a role within the Command, Numbered AF, Wing, Group, or Squadron. This IMA Officer or NCO would bring their experience regarding cyber into the units, leading to the development of cyber knowledge at operational units and building relationships within the cyber and combat forces communities.

The TR typically serves fourteen days a year, annual training, and monthly for 2-day weekend drill periods. The TR maintains currency, qualification, and most of all, recencies in their specialty. They typically are well seasoned in their specialty and therefore fit best into staff or tactical-level units. They can also operate using Mobilization Period Augmentee (MPA) periods. TRs fill operator roles and augment active units or manage their own. The advantage of these reservists is that they are "true" Citizen Airmen, trained to support operational and tactical functions. Enabling individuals to acquire the skills necessary for success in the cyber-civilian workforce, transition into that workforce, and subsequently bring back civilian tradecraft to enhance our military organization, contributes to building enduring civ-mil relationships beyond the defense sector—a strategic success for the DOD in the long run.

A Bridge of Skill Sets and Leadership: Skilled Airman

A third use of cyber reserve officers is blended cyber officers, in which the force retains talented officers and NCOs from other specialties by retraining them as reserve cyber officers. Capturing their valuable leadership experience, retaining talent, diversifying skills, and establishing a cyber-to-conventional forces feedback loop, resulting in better cyber-conventional force integration. Such officers or NCOs can be IMAs or TRs, but best fit the TR role, specifically as leadership. Examples of such talent capture are Pilots, Air Battle Managers, and Combat Systems Officers. These personnel bring extensive planning and operational experience, an understanding of culture, and key specialty experience to the cyber force. Many of these personnel want to continue to serve after leaving their active-duty roles; however, they want to do so in a different capacity. Therefore, this is a chance to retain critical experience and bolster our cyber force integration into traditional domains: air, land, and sea. This unique path would utilize a cyber top-off course or initial qualification training to build an understanding of the career field. The intent is not to utilize these officers as operators but as leaders, integrators, and liaisons.

Blended Officer an Example of Retention Capture:

As many aviators approach the end of their Active-Duty Service Commitment (ADSC), they must determine a path forward. These officers have had extensive military training and experience that takes years to recapture. For example, an EC-130 Electronic Warfare Officer (EWO) is finishing his or her 8th year in service and when they reach this crossroads. After 2.5 years of formal training and 5.5 years of deployments and Temporary Duty (TDY), they concluded that they would like to pursue a non-military career. This officer, though, possesses security clearances, leadership experience, extensive training, and exposure to Joint Force Operations. Perhaps most importantly, the USAF will retain an in-depth background in

Electronic Warfare (EW) and Aerial Warfare. One mission, EW, is actively utilized in cyberspace and is directly transferable. Additionally, the background in Aerial Warfare, directly supported by cyber, gives this Captain unique qualities to work as a liaison between operational flying units and the cyber forces that enable them to function. Therefore, this results in a more cohesive force that draws upon an officer's experience. As explained previously, this officer may need a short top-off course to familiarize him or her with the cyber force structure and enterprise, followed by an assignment to a supporting unit for his or her drill period. It has resulted in the capturing of talent for the DOD and the ability for the officers to continue their service, built on their retirement benefits, acquisition of low-cost healthcare, and access to opportunities outside of the civilian workforce.

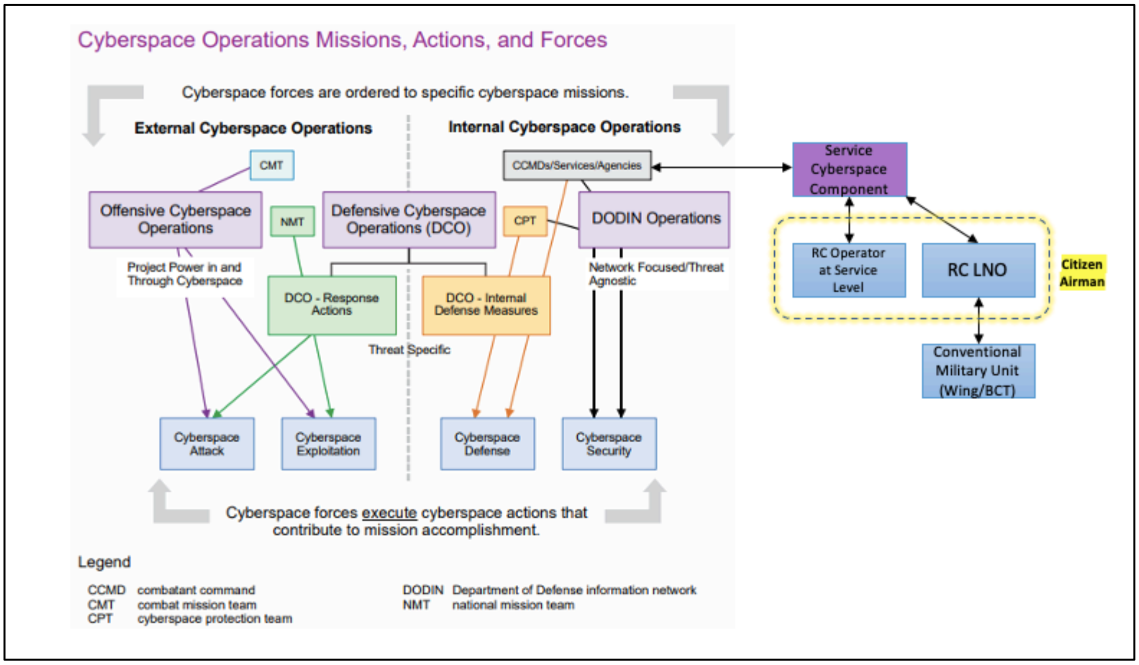
Cyberspace Operations Missions, Actions, and Forces
Cyberspace forces are ordered to specific cyberspace missions.
External Cyberspace Operations
Internal Cyberspace Operations
CMT
CCMDs/Services/Agencies
Offensive Cyberspace Operations
NMT
Defensive Cyberspace Operations (DCO)
CPT
DODIN Operations
Project Power in and Through Cyberspace
DCO - Response Actions
DCO - Internal Defense Measures
Network Focused/Threat Agnostic
Threat Specific
Cyberspace Attack
Cyberspace Exploitation
Cyberspace Defense
Cyberspace Security
Cyberspace forces execute cyberspace actions that contribute to mission accomplishment.
Legend
CCMD combatant command
CMT combat mission team
CPT cyberspace protection team
DODIN Department of Defense information network
NMT national mission team
Service Cyberspace Component
RC Operator at Service Level
RC LNO
Citizen Airman
Conventional Military Unit (Wing/BCT)

Fig. 2 Cyberspace operations missions, actions, and forces (image reprinted from Joint Publication 3-12, modified)[16]

Civilian Expertise Required: An Aeromedical Success, Applicable to Cyber

Much like the Cyber Force, the medical career field seeks greater pay outside the military. Additionally, both career fields get more exposure, reps, and increased opportunities to learn or sharpen skills in the civilian sector. By serving in the Air Force Reserve, these healthcare professionals can continue their civilian careers and serve their country." [17] The continuous exposure to more extensive medical facilities and trauma cases allows these reserve personnel to be the sharpest and most experienced medical members. This gained experience is, in the Reserves, particularly on display in the aeromedical team, which is a mission that the Air Force Reserve provides 80% of the total aviation personnel and approximately 65-70% of the total Air Force Critical Care Air Transport Teams (CCATT).[18] These reservists often bring new techniques and lessons learned to the active component. The capability of these Airmen to save lives is exceptionally crucial. The aeromedical evacuation mission has drastically evolved from a primarily active component mission, in which combat-to-stateside treatment averaged thirty days during Vietnam, to the contemporary, predominately reserve component mission, which has resulted in a combat-to-stateside treatment average of less than three days.[19] Resulting in a 98% survival rate of theater causalities and demonstrating the potential of a well-managed and utilized reserve component. [20]

Conclusion

In conclusion, we must first and foremost consider the warfighters and their cyber competency. Most warfighters across the domains need to learn how to engage with cyber or how cyber helps them beyond the wavetop. Currently, there are few or no personnel tasked to engage routinely with the combat forces across the services, below the staff of the combatant or geographic command. This leads to limited cohesion at the tactical level of cyber and conventional forces, as well as results in an ambiguous transition of tactical cyber and strategic cyber supported or in support of conventional forces. Consider the role of the Air Liaison Officer to the Army at each echelon (Brigade, Division, Battalion, etc.). These Air Force officers are crucial to the joint fight and enable tactical air control for close air support. Such liaison and integration are just as crucial for cyber, and we must integrate this domain. The reserve component and geographic alignment can resolve this shortcoming in integration. Second, centers of power must align with the civilian workforce and be geographically centered. USCYBERCOM and the NSA are by far the overwhelming center of the cyber force. These installations are, for example, centered in one geographic area, Fort Meade, Maryland, far from most of the civilian IT and INFOSEC workforce. Third, the military struggles with recruiting and retaining talent, more so retaining it. The military can solve this by geographically centering in the civilian areas and focusing on retaining talented individuals like the USAF 17S specialty, who are often the "most talented and technically competent members" of the USAF cyber force and are "…being lost at high rates."[21]

The reserve component is uniquely positioned to capture this exodus. Allowing members to leave, establish new careers, obtain new skills, and yet, through their reserve role, feedback to the overall force's integrity and strengths, as proven successful by the Aeromedical Mission and the Citizen Airmen who made this success possible.

This paper is dedicated to Maddi Dagenhart whose love and support fueled my journey at Air Command Staff College.

[1] Piret Pernik, "Preparing for Cyber Conflict: Case Studies of Cyber Command" (Tallinn, Estonia: International Centre for Defence and Security, 2018). p.2-3

[2] Air Force Doctrine Publication, Cyberspace Operations (2023), p.1.

[3] Lara Schmidt et al., Cyber Practices: What Can the U.S. Air Force Learn from the Commercial Sector? (Santa Monica, CA: RAND Corporation, 2015). p.xi

[4] Air Force Doctrine Publication, Cyberspace Operations (2023), p.4.

[5] Schmidt et al., Cyber Practices: What Can the U.S. Air Force Learn from the Commercial Sector?, RAND Corporation, 2015, https://www.rand.org/pubs/research_reports/RR847.html, p. xi-xii.

[6] Ibid p. 33.

[7] Ibid p. xiii-xiv

[8] Porche, Isaac R., III, et al. "Cyber Power Potential of the Army's Reserve Component." RAND Corporation, RR-1490, 2017. p. 27

[9] Ibid p.27.

[10] CBRE, "Scoring Tech Talent 2022" (2022), https://www.cbre.com/insights/books/scoring-tech-talent-2022.

[11] Ibid

[12] Robin G. Sneed and Robert A. Kilmer, "The Air Force's Individual Mobilization Augmentee Program Is the Current Organizational Structure Viable?" Air & Space Power Journal 26, no. 5 (2012): 13.

[13] Ibid p.13

[14] Ibid p. 14-15.

[15] Department of Defense, "About the Reserve Link," 2010, http://www.af.mil/reservelink/about/about_us.asp, p. 4.

[16] Joint Chiefs of Staff, Cyberspace Operations, Joint Publication No.: JP 3-12, December 19, 2022, https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/. p.17

[17] Department of Defense, "About the Reserve Link," 2010, http://www.af.mil/reservelink/about/about_us.asp, 7.

[18] Air Force Medical Service, "AFMS Capability: Critical Care Air Transport Team," 2023, https://www.airforcemedicine.af.mil/Platforms/AFMS-Capability-Critical-Care-Air-Transport-Team/.

[19] Ibid

[20] Joint Base Charleston Public Affairs, "Aeromedical evacuation: Helping the wounded survive the journey home," 2023, https://www.jbcharleston.jb.mil/News/Article-Display/Article/236867/aeromedical-evacuation-helping-the-wounded-survive-the-journey-home/.

[21] Chaitra M. Hardison et al., "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, 9.

Bibliography

Air Force Doctrine Publication. "Cyberspace Operations." 2023.

Air Force Medical Service. "AFMS Capability: Critical Care Air Transport Team." 2023. Retrieved from https://www.airforcemedicine.af.mil/Platforms/AFMS-Capability-Critical-Care-Air-Transport-Team/.

CBRE. "Scoring Tech Talent 2022." 2022. Retrieved from https://www.cbre.com/insights/books/scoring-tech-talent-2022.

Department of Defense. "About the Reserve Link." 2010. Retrieved from http://www.af.mil/reservelink/about/about_us.asp.

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. Retrieved from https://www.rand.org/pubs/research_reports/RR2618.html.

Joint Base Charleston Public Affairs. "Aeromedical evacuation: Helping the wounded survive the journey home." 2023. Retrieved from https://www.jbcharleston.jb.mil/News/Article-Display/Article/236867/aeromedical-evacuation-helping-the-wounded-survive-the-journey-home/.

Joint Chiefs of Staff. Cyberspace Operations. Joint Chiefs of Staff (US), December 19, 2022. Joint Publication No.: JP 3-12. Retrieved from https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/.

Pernik, Piret. Preparing for Cyber Conflict: Case Studies of Cyber Command. Tallinn, Estonia: International Centre for Defence and Security, 2018.

Porche, Isaac R., III, et al. "Cyber Power Potential of the Army's Reserve Component." RAND Corporation, RR-1490, 2017.

Schmidt, Lara, Caolionn O'Connell, Hirokazu Miyake, Akhil R. Shah, Joshua Baron, Geof Nieboer, Rose Jourdan, David Senty, Zev Winkelman, Louise Taggart, Susanne Sondergaard, and Neil Robinson. Cyber Practices: What Can the U.S. Air Force Learn from the Commercial Sector? Santa Monica, CA: RAND Corporation, 2015. Retrieved from https://www.rand.org/pubs/research_reports/RR847.html.