Identifying Enlisted Recruits With the Right Stuff to Perform Cyberspace Operations

Thomas Barth, Elizabeth McDaniel

The Challenge: Identifying enlisted personnel for the cyberspace effects workforce is challenged by a shallow pool of candidates and steep qualifying and performance requirements. If the Army can identify recruits with the right attributes and potential, it can increase the number who pass lengthy and expensive advanced training.

There are only so many people with cyber skills to begin with. It may take ten years to grow the pool to a sufficient number of qualified candidates.

According to the Department of Defense (DoD) Strategy for Operating in Cyberspace, "The development and retention of an exceptional cyberspace workforce is central to DoD's strategic success." (DoD Strategy for Operating in Cyberspace January 2011) The supply and demand imbalance has been well documented:

> *There are only so many people with cyber skills to begin with. It may take ten years to grow the pool to a sufficient number of qualified candidates. The pool for the DoD is especially shallow due to the requirements for U.S. citizenship, clean credit, and the ability to obtain a clearance. (Private sector security executive n.d.)*

DoD's cyberspace workforce comprises personnel assigned to the areas of cyberspace effects, cybersecurity, cyberspace IT, and portions of the Intelligence workforces. (DoD Directive 8140.01) Developing the cyberspace effects workforce, the "personnel who plan, support, and execute cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in and through cyberspace," (DoD Directive 8140.01) presents a particularly difficult set of challenges. To meet its requirements for the Cyber Mission Force (CMF) teams, a component of the cyber effects workforce, the Army is recruiting individuals to serve as cyber operations specialists, classified as military occupation specialty (MOS) 17C. Cyber operations specialists execute defensive and offensive cyberspace operations. Their duties include performing cyber-attacks and defenses; performing cyber intelligence, surveillance, and reconnaissance actions on specified systems and networks; conducting network terrain audits, penetration testing, basic digital forensics data analysis, and software threat analysis; reacting to cyberspace events; employing cyberspace defense

infrastructure capabilities; collecting basic digital forensics data; providing incident response impact assessments; and producing network security posture assessments. The training process for cyber operations specialists requires the successful completion of 10 weeks of Basic Combat Training and two phases of Advanced Individual Training (AIT), plus an additional 45 weeks of intense technical cyber training. (U.S. Army 2017)

The funnel below illustrates the challenge facing the Army in identifying and recruiting a pool of enlisted personnel who can complete successfully the intensive training process and join its cyber mission teams as qualified cyber operations specialists.

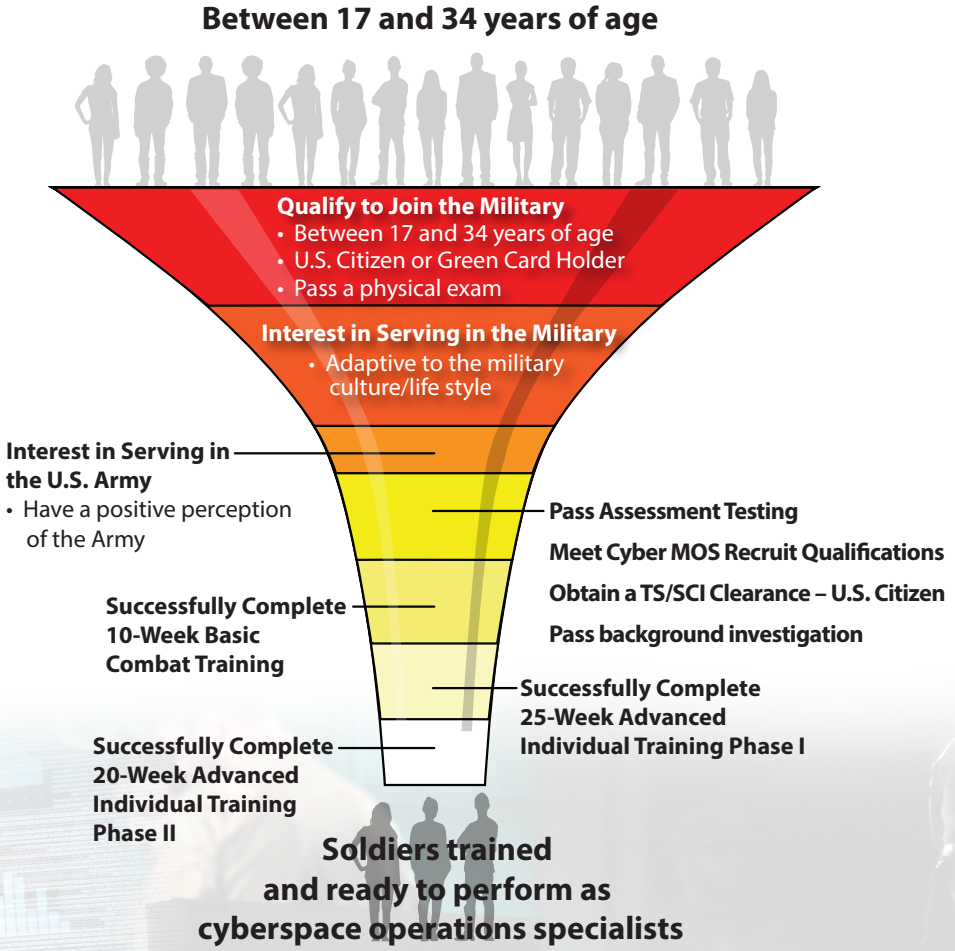
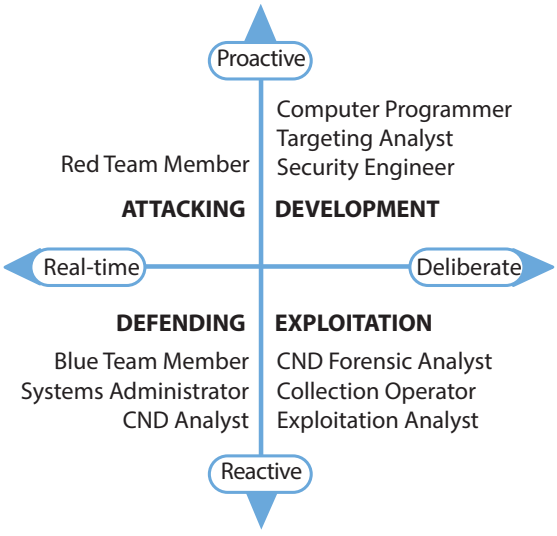


Figure 1. A Notional Funnel to Illustrate the Army's Challenge in Identifying and Training the Enlisted Recruits for Cyberspace Operations Roles.

Efforts to Assess the Aptitudes of Recruits for the Cyber Workforce

Since the 1940s, the U.S. Armed Services have explored the use of personality variables as predictors of performance. At a Military Entrance Processing Station (MEPS), a prospective recruit currently takes a battery of tests to assess his or her general and specific knowledge and aptitude for a variety of MOSs. The Armed Services Vocational Aptitude Battery (ASVAB) qualifies applicants to enlist in the military and assigns them to particular jobs and fields. Its tests measure aptitudes in four domains: verbal, math, science and technical, and spatial. OCCU-Find, an inventory of work-related interests, is part of the ASVAB Career Exploration Program for recruits.

Since the 1950s, the Services have explored the relationships among work interest and preferences, motivation, identity, meaningfulness, sense of belonging, and work-related behavior. (Campbell, O'Rourke and Bunting 2015) The Cyber Test (CT), originally called the Information and Communication Technology Literacy (ICTL) Test, has been administered as an operational test to Service applicants since 2014. The intent of the CT is to assist DoD stakeholders in selecting and classifying enlisted personnel likely to be successful in training for a range of entry-level technology-related occupations. The CT is administered at MEPS on the ASVAB platform to Service applicants who wish to pursue select information technology (IT)/ cyber careers. The CT is modeled after an ASVAB information test (e.g., Electronics Information) and assesses basic computer literacy via knowledge-based multiple-choice questions in four fundamental areas: computer operations, networks, security and compliance, and software programming. The CT has demonstrated potential to improve the quality of applicants and reduce academic turnover in technical training for these demanding occupations. (Correspondence with Michael Ingerick 2017) The Cyber Aptitude and Talent Assessment (CATA), developed by the University of Maryland's Center for Advanced Study of Language (CASL), focuses on attributes with predictive value for cyber tasks. As illustrated in Figure 2, the roles are segmented to match the demands of particular tasks along two dimensions: proactive to responsive, and real-time to deliberate. (Campbell, O'Rourke and Bunting 2015)



CND = Computer Network Defense

Source: Campbell, O'Rourke and Bunting 2015

Figure 2. Cyber Roles Differ along Two Dimensions.

In 2016, CASL partnered with the Air Force to develop the AF-CATA, which focuses on critical thinking and other foundational abilities for success in cyber warfare operator training, including working memory and spatial visualization, as well as traits that predict operational job performance, like speed and vigilance. (Campbell, Identifying Untapped Talent 2017) The Canadian Armed Forces and the UK Ministry of Defence are currently using the Defence Cyber Aptitude Test developed by IBM to identify personnel with natural talent and the right skills for specific cyber positions. (Davies 2017)

Research continues on the predictive value of other assessments on attributes related to cyber roles. One is the Tailored Adaptive Personality Assessment System (TAPAS), which the Army has been administering at MEPS since 2009. Also, the U.S. Army Research Institute for the Behavioral and Social Sciences is developing the Common Cyber Capabilities Test, to measure the five to seven capabilities determined to be important to cyber work, and the Systems Thinking Assessment. (Wind 2017)

Characteristics of Personnel Who Might Fill Cyber Roles

Hackers, Red Teamers, and Pen Testers

In the media, the term "hacker" is used to describe a cybercriminal; however, the Army focuses on the ethical kind. Possessing exceptional talents, passions, and proclivities for highly specialized cyber roles, these skilled professionals know how to look for weaknesses in networks and/or computer systems. They are needed to maintain national security and protect our nation's critical infrastructure. They are characterized by high intelligence, consuming curiosity, and facility with intellectual pursuits. (Department of the Navy 2017)

Hackers called *Red Teamers*, or intrusion or pen (penetration) testers, conduct vulnerability probes of an organization's computer networks (with the organization's consent) to discover vulnerabilities and provide remedial solutions to make the networks and systems more secure and safe.

Ethical hackers are cyber security/effects professionals who demonstrate their skills as Red Team members or penetration testers in support of the mission of the organization. The Certified Ethical Hacker (CEH) certification can be earned through assessment of one's knowledge of the security of computer systems using penetration testing techniques. (EC-Council 2017)

Cyber Warriors

Cyber warriors use cyber weapons, strategies, and technologies for nonmilitary ends such as cyber espionage. They tend to be well trained and educated, with approximately one half possessing at least a bachelor's degree. (Beard 2016) The Offensive Security Certified Professional (OSCP) is available only to those who conduct offensive operations and have passed specific training and a 24-hour online examination. (Offensive Security

2017) According to one private sector cyber executive, the OSCP is essential for acceptance as a colleague by some critical cyber operations teams.

Cyber warriors often demonstrate skills such as network traffic sniffing, packet analysis, network and system mapping, forensics, reverse engineering, binary analysis, and other such capabilities. (Andress and Winterfield 2014) In their capacity as warriors, their age and physical fitness are less critical than in traditional combat roles; however, they must be able to sit for long periods of time in front of computers. Mental factors such as maturity, intelligence, problem-solving skills, and creativity are highly valued, but among this population resistance to rules and authority figures may be common. They are intensely curious about how things work and can be made to fail. Cyber warriors, serving in critical roles, must demonstrate such qualities as self-control, empathy for the noncombatant population, temperance against the temptation to do what is expedient rather that what is right, discretion and discernment regarding privacy, and honor, among other attributes. (Beard 2016)

According to the authors of *The Human Side of Cyber Conflict: Organizing, Training, and Equipping the Air Force Cyber Workforce*, a key to force structure is finding educated people with a proclivity toward hacking. Interest and competence in science, technology, engineering, and mathematics (STEM) fields does not necessarily mean an individual might be a good cyber operator. Higher education is critical for success in performing some cyber warfare roles due to their reliance on theoretical as well as practical education. Graduate work develops the minds of individuals with technical aptitude to apply their knowledge of cyberspace to research, design, develop, test, and evaluate hardware, software, and firmware for the purpose of exploiting, defending, and attacking cyber and cyber physical systems. Training without education proved insufficient to assure mathematically complex, information-centric systems. If the Air Force identifies a candidate for a certain cyber operations role who has high aptitude or proclivity who lacks the required degree, such as a bachelor's degree in computer science, the Air Force might make an exception until the degree is earned. (Yannakgeorgos and Geis 2016)

Continuing Efforts

The Army continues to investigate the link between aptitude, knowledge and skill, maturity, personality traits, and motivation with successful performance in cyber operations roles of new recruits and enlisted personnel already in the force. Further research is needed to link attributes identified by CT and CATA and the performance of personnel in cyber operations roles in the Army and other Military Services, as well as the predictive value of CT and performance in the Joint Cyber Analysis Course (JCAC) and the Army Research Institute's development of new instruments.

References

Andress, J., and S. Winterfield. 2014. *Cyber Warfare, Second Edition: Techniques, Tactics, and Tools for Security Practitioners*. Waltham, MA: Elsevier.

Beard, M. 2016. "Beyond Tallinn: The Code of the Cyberwarrior?" In *Binary Bullets: The Ethics of Cyberwarfare*, edited by F. Allhof, A. Henschke and B. J. Strawser. New York: Oxford University Press.

Campbell, Susan G. 2017. "Identifying Untapped Talent for Cyber Warfare Operations Using a Cyber Aptitude and Talent Assessment," *NICE 2017 Spring eNewsletter*." https://www.nist.gov/itl/applied-cybersecurity/nice/nice-2017-spring-enewsletter#Featured.

Campbell, Susan G., Polly O'Rourke, and Michael F. Bunting. 2015. "Identifying Dimensions of Cyber Aptitude: The Design of the Cyber Aptitude and Talent Assessment." *Proceedings of the Human Factors and Ergonomics Society 59th Annual Meeting*.

2017. Correspondence with Michael Ingerick (The Human Resources Research Organization). September 5.

Davies, N. 2017. "Davies, N., "Cyber Aptitude in the Military," *Frontline Defence* 14 (3). http://defence.frontline.online/article/2017/3/7065-Cyber-Aptitude-in-the-Military.

Department of the Navy. 2017. "Credentialing Opportunities Online (COOL)." April 3. https://www.cool.navy.mil/

Department of Defense. 2017. "DoD Directive 8140.01, Cyberspace Workforce Management." July 31.

Department of Defense. 2011. "DoD Strategy for Operating in Cyberspace." January.

EC-Council. 2017. "Certified Ethical Hacking Certification." https://www.eccouncil.org/Certification/certified-ethical-hacker.

Offensive Security. 2017. "Offensive Security Certified Professional." https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/.

Private sector security executive, interview by IDA. n.d.

U.S. Army. 2017. "Careers & Jobs: Cyber Operations Specialist (17C)." August 22. https://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/computers-and-technology/cyber-operations-specialist.html.

Interview with Dr. Alexander P. Wind, Army Research Institute for Behavioral and Social Sciences. 21 January 2016.

Yannakogeorgos, P. A., and J. P. Geis. 2016. *The Human Side of Cyber Conflict: Organizing, Training, and Equipping the Air Force Cyber Workforce*. Maxwell Air Force Base, Alabama: Air University Press: Air Force Research Institute.

Mr. Thomas Barth is a Research Staff Member in IDA's Information Technology and Systems Division. He holds a Master of Arts in strategic studies from the U.S. Army War College and a Master of Arts in military art and science from the School of Advanced Military Studies, U.S. Command and General Staff College.

Dr. Elizabeth McDaniel is an Adjunct Research Staff Member in IDA's Information Technology and Systems Division. She holds a Doctor of Philosophy in education from the University of Miami.