Cyber Aptitude Assessment – Finding the Next Generation of Enlisted Cyber Soldiers

MSG Jeffrey D. Morris, USA and CPT Frederick R. Waage, USA

DEPARTMENT OF THE ARMY
UNITED STATE MILITARY ACADEMY

ARMY CYBER INSTITUTE
West Point, New York

The views expressed in this work are those of the authors and do not reflect the official policy or position of the United States Army, Department of Defense, or the United States Government. This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

Contents

Executive Synopsis

The Department of Defense (DoD), and the US Army, are rapidly expanding the positions and personnel to operate in the cyberspace domain, one of the five independent warfighting domains [1]. Recognizing the importance of integrating cyber operations throughout the Army led to the recent creation of a new cyber branch, the first new branch in decades. Filling these new positions with the best qualified personnel is not an easy task.

The DoD Cyberspace Workforce Strategy of 2013 lays outs requirements to assess aptitude and qualifications, noting "not all successful cyberspace personnel will have a Science, Technology, Engineering and Math (STEM) background. Rather, a broad range of experiences can lead to a qualified cyberspace employee." The Strategy directs developing aptitude assessment methods to identify individuals' thinking and problem-solving abilities as tools for recruitment. Further, it directs DoD to evaluate the "availability or development" of assessment tools to identify military candidates for cyberspace positions. [2]

This paper begins with a discussion of the issues surrounding aptitude assessment and continues by identifying several existing test instruments. It then   identifies testing results and finishes with several recommendations for talent identification.

Introduction

As noted in the 2003 DoD Cyberspace Workforce Strategy, not all cyberspace personnel will have a STEM background, but instead will come from a broad variety of backgrounds [2]. The problem is trying to find personnel having the knowledge and aptitude for cyberspace operations. There are many instruments available to measure knowledge, but there few that measure aptitude.

The traditional military approach of over-selecting numbers of personnel for training to fill requirements may not be the best approach for cyberspace forces. Selecting the right personnel and investing in them will be as important as investing in the correct hardware and software [3]. While making progress in selecting and filling cyber positions, the DOD is steadily losing ground. General Keith Alexander (former head of the USCYBERCOM) noted in 2013 "[USCYBERCOM's] progress, however, can only continue if we are able to fulfill our urgent requirement for sufficient trained, certified, and ready forces to defend U.S. national interests in cyberspace" [2].

The challenge is identifying the right people for the job. There is some agreement that developed cognitive problem-solving is a desired trait for cyber personnel, but there is much argument on how to measure if a candidate has it. The traditional testing method for military accessions does not properly test for desired cyber traits. These needs suggest the military requires different methods and authorities for filling the cyber force [4, 5].

The 2003 DoD Cyberspace Workforce Strategy suggests employing a multi-dimensional, innovative approach to recruiting, by assessing aptitude and helping to create a "national cyberspace talent pipeline" [2]. This approach needs to evaluate cognitive talents tied to the various cybersecurity jobs identified by the National Institute for Cybersecurity Education (NICE), which are organized by mission function [6]. Rather than measuring current knowledge, the assessment needs to look for factors affecting an applicant's aptitude and potential success in cyber operations [7].

Potential cyberspace personnel fall into two categories: new accessions into the military and current military personnel requesting assignment to cyberspace operations. New accessions come from a background where computers and computing devices are commonplace and many are "digital or net natives" that have grown up surrounded by the Internet and digital communication devices. Many have become accustomed to teaching the older generation how to use current technology. This is a reverse of the typical paradigm considering young individuals as amateurs or students [5].

Current military personnel wanting to move into cyber careers are another challenge for identifying potential cyber personnel. Personal interest in cyber motivates many of these personnel, rather than military training. Finding those with the aptitude for cyber, rather than technical qualifications, needs a different assessment, but would expand the pool of available talent [2].

Discussion of Testing Instruments

This section describes several existing aptitude tests identified during a literature search. Each subsection describes what the test measures, the potential test population, background information about the test, and who created the test. Supporting statistics and information further explains the details of the test.

CATA (Cyber Aptitude and Talent Assessment)

The CATA is a test created by the University of Maryland Center for Advanced Study of Language (CASL) based on their experience in creating a second-generation version of the Defense Language Aptitude Battery (DLAB). The DoD Cyberspace Workforce Strategy produced in 2013 directs the DoD to evaluate assessments to augment or replace existing tools by using the DLAB as *one of the models* for an aptitude assessment.

The document does not specify using a DLAB-based assessment, only perform the evaluation using the DLAB as a basis.

The CATA is designed to predict cyber aptitude beyond assessing general intelligence. The CATA model uses classification of jobs requiring deliberate performance or action and proactive and reactive actions. Deliberate action is a combination of critical thinking ability and the ability to defer resolution. Their model of cybersecurity performance consists of two components: critical thinking and measurement of constructs that match particular cybersecurity jobs [8]. The CATA is designed to assess discrete cognitive skills identified as key to categories identified in a cybersecurity job model designed by CASL. See Figure 1 for a graphic showing the four dimensions of the CASL model.

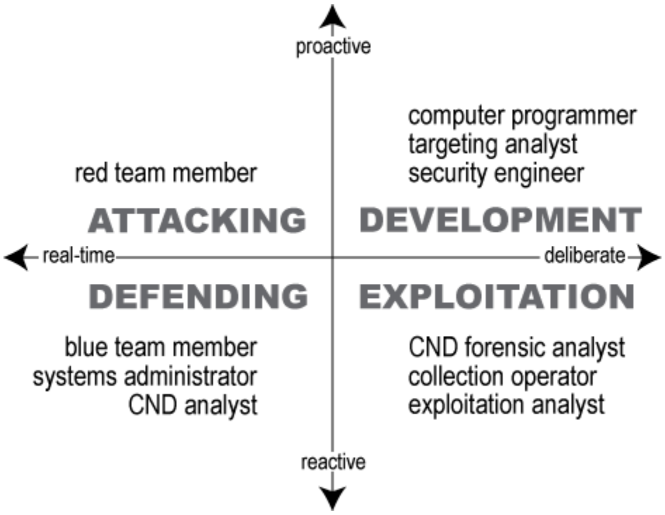


Figure 1. Schematic of the dimensions on which example cyber careers differ. The quadrant names (in bold uppercase font; e.g., ATTACKING) correspond to a major job task that has the characteristics described on its axes (for instance, “defending” requires real-time reaction, while “development” requires proactive deliberation). Example job titles, which appear within quadrants, are taken from the NICE framework [8].

CASL suggests measuring different aspects of critical thinking, based on their review of predicted performance indicators in computer science and STEM occupations. The CATA measures: visuospatial working memory, rule induction, complex problem-solving, spatial visualization, and attentional capacity. The CATA design does not assess written or verbal skills because they are assessed using the Armed Services Aptitude Battery (ASVAB) or an interview process [8]. Table 1 lists the proposed content of the CATA.

Table 1. Proposed content of the CASL's CATA, section, construct, and proposed test to measure that construct. See [6] for a detailed description of each section and test.

Section	**Construct**	**Test**
Critical Thinking	Visuospatial Working Memory	Shapebuilder
	Rule Induction	Letter Sets
	Complex Problem-Solving	Dynamic Systems Control
	Spatial Visualization	Paper Folding
	Attentional Capacity	Shape Comparison
Deliberate Action	Need For Closure	Need For Cognitive Closure
	Tolerance For Risk	Balloon Analogue Risk Task
Real-Time Action	Psychomotor Speed	Recent Probes (1 item)
	Pattern Recognition and Scanning	Decoding Speed
	Resistance To Interference	Recent Probes (4 & 9 Items)
Proactive Thinking	Modeling Program Execution	Spatial Integration
	Creativity	Remote Associates Test
Reactive Thinking	Anomaly Detection	Anomalous Behavior Test
	Vigilance	Pattern Vigilance

ASVAB – Cyber Test (CT) (Formerly the Information Communications Technology Literacy test (ICTL))

The Information/Communication Technology Literacy (ICTL) (now known as the Cyber Test (CT)) began as a request by the Office of the Assistant Secretary of Defense to the Defense Manpower Data Center to review of the ASVAB in 2005. There were concerns the ASVAB content was outdated due to rapid changes in computer technology throughout the military. Accelerating these changes were continuing combat operations and an increasingly computer-centric form of warfare. Also, the services needed to identify characteristics needed for military personnel to use these new systems [9].

The CT is a cognitive measure designed as an ASVAB technical subtest to predict training performance in entry-level cyber-related military occupations. The CT in an information test, much like the ASVAB technical subtests, and thought to be an indirect measure of "of interest, intrinsic motivation, and skill in a particular area" [10]. The test is expected to have a strong relationship with cyber-related tasks or course grades, but may be an indirect indicator of finding the best Military Occupational Specialty (MOS) for a particular applicant (i.e. "MOS fit") [10].

These information tests have a successful history of use as far back as the Army Air Forces Aviation Psychology Program during World War II. Several key characteristics for information tests include [11]:

- Indirect measures of interest, motivation, aptitude, and skill in a particular area.
- Not intended to certify an individual at a particular skill level or identify who does not need training (they are not 'certification tests').

- Assess knowledge and skill at a general level and provided an objective measure of interest and motivation in a technical content area.
- Information or knowledge items as useful predictors of performance in training for related jobs.

Information tests like the Automotive Information test, an ASVAB technical subtest, help identify people who like to work on vehicles and therefore are more likely to be a better fit to an automotive related MOS (e.g., Light Wheel Vehicle Mechanic). The CT is designed to identify those who like functioning in the information technology fields, and may have an aptitude for training and operations in military cyber-related occupations [10].

A major requirement for the CT was it needed to provide incremental validity beyond the ASVAB. In other words, it had to be provably better than the ASVAB at selecting successful cyber personnel, with ‘success’ defined as passing military entry-level cyber training. Previous evidence showed the ASVAB is a good test of aptitude for several constructs such as math and verbal aptitude, so the CT focused on areas not already measured by the ASVAB [11]. The CT included a Figural Reasoning test taken from the Enhanced Computer-Administered Test battery with Subject Matter Experts (SMEs) suggesting nonverbal reasoning is important for cyber jobs [12]. Note that previous military research suggests even small amounts of incremental validity can have utility in large selection programs [10].

The US Air Force became the lead service for development of an additional test for the ASVAB. The Air Force selected the Human Resources Research Organization to develop and validate the then-labeled ICTL test [10]. The research program has comprised multiple phases and included: (a) review and integration of existing taxonomies, (b) interviews with military cyber/IT SMEs, and (c) online survey of additional military IT SMEs to evaluate and adapt the initial taxonomy based on definitions of abilities for cyber and information technology operations. See Table 2 for the definitions.

Table 2. Definitions of Abilities for Cyber/IT Operations [12]

Ability	Definition
Verbal reasoning	Ability to solve verbal/word problems by reasoning logically
Nonverbal reasoning	Ability to solve nonverbal problems (graphical, puzzles, and diagrammatic) by reasoning logically
Mathematical reasoning	Ability to reason mathematically and choose the right mathematical methods or formulas to solve a problem
Problem sensitivity	Ability to tell when something is wrong or is likely to go wrong. It does not involve solving the problem, only recognizing there is a problem
Originality	Ability to come up with unusual or clever ideas about a given topic or situation or to develop creative ways to solve a problem
Information ordering	Ability to arrange things or actions in a certain order or pattern according to a specific rule or set of rules (e.g., patterns of numbers, letters, words, pictures, mathematical operations)
Written communication	Ability to read and understand information and ideas presented in writing
Oral comprehension	Ability to listen to and understand information and ideas presented through spoken words and sentences
Perceptual speed	Ability to quickly and accurately compare similarities and differences among sets of letters, numbers, objects, pictures, or patterns
Advanced written comprehension	Ability to read and understand technical and/or government documents
Written expression	Ability to communicate information and ideas in writing so others will understand
Near vision	Ability to see details at close range (within a few feet of the observer)

Cyber Talent Enhanced – SANS

The Cyber Talent Enhanced (CTE) is a combined aptitude/skills exam from the SANS organization. The test is designed to determine both aptitude for cyber operations and assess the current skill set of the test taker based on the SANS set of cyber training. The potential outcome is an assessment of the examinee’s aptitude for cyber and a suggested list of SANS training for the candidate. The exam is a two-hour assessment completed online through a web-based interface. The current version of the test contains an equal portion of aptitude and skill assessment questions [13].

A small sample set (<20 individuals) took the exam in the fall of 2013 as a pilot program with Army MOS 25D personnel. Initial results showed some positive correlations, leading to larger test group in the summer of 2014. This test group, while larger than the first (~40 individuals), was still limited compared to the much larger ICTL test group and there is little testing data available as the test and corresponding results are proprietary property of SANS [13]. There is current proposal from SANS to provide a limited number of the assessment for continued testing for small groups of students.

The Cyber Talent Targeting Methodology (CTI)

The strength of the Cyber branch is the diversity of its collective talents derived from the unique experiences and technical expertise of its individuals spread across multiple demographic groups. Thus, the Army should target ‘high-value individuals with cyber talent to join its cyber ranks rather than a specific demographic group or formation. To paraphrase Army Techniques Publication 3-60 (Targeting) [14], high-value individuals are people of interest that targeteers must first identify, then track, and engage.

One methodology employed by the Army to target such individuals is the Find, Fix, Finish, Exploit, Analyze, and Disseminate (F3EAD), which is a “technique that works at all levels for leaders to understand their operational environment and visualize the effects they want to achieve” [14]. Finding targetable cyber talent is similar to finding the exact location of “a HVI in the midst of civilian clutter”; however, finding the “accurate location enables surgical finishing effects that emphasize speed to catch a mobile target” [14]. The Army could modify the F3EAD targeting process to identify and manage its cyber talent into Find, Fix, Finish, Exploit, Steady-state, and Assess (F3ESA). The F3ESA Cyber Talent Targeting process is two phased with phase one focusing on CTI and phase two focused on Cyber Talent Management (CTM). Cyber Branch can apply F3ESA in acquiring both non-cyber Soldiers internally from the Army and external candidates from commercial, joint, inter-agency, and academic populations. The remainder of this section will focus on phase one. See Figure 2 for the Cyber Talent Targeting Methodology.

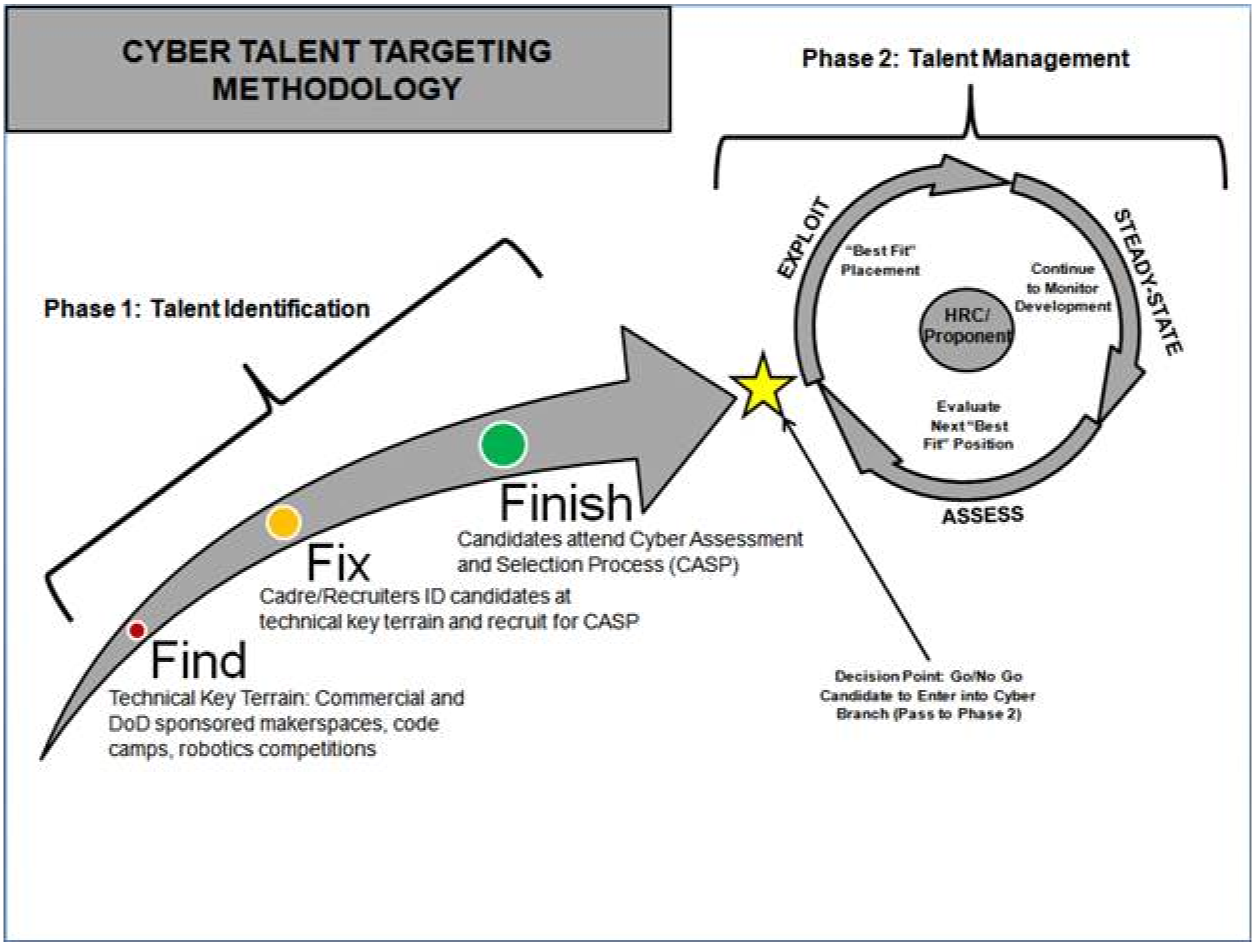

CYBER TALENT TARGETING METHODOLOGY
Phase 2: Talent Management
Phase 1: Talent Identification
EXPLOIT
STEADY-STATE
ASSESS
"Best Fit" Placement
Continue to Monitor Development
HRC/ Proponent
Evaluate Next "Best Fit" Position
Finish
Candidates attend Cyber Assessment and Selection Process (CASP)
Fix
Cadre/Recruiters ID candidates at technical key terrain and recruit for CASP
Find
Technical Key Terrain: Commercial and DoD sponsored makerspaces, code camps, robotics competitions
Decision Point: Go/No Go Candidate to Enter into Cyber Branch (Pass to Phase 2)

Figure 2. Proposed Cyber Talent Targeting Methodology that is modified from the F3EAD targeting process.

FIND PIECE: Identify Key Technical Terrain Where Cyber Talent Converges

Cyber talent weaves intermittently throughout multiple demographic sub-groups. For CTI efficiency, the Army must conduct a “pattern-of-life analysis” to identify technical venues where cyber talent congregates. One may infer many of the individuals who tend to these technical congregation points are mavens motivated by an intrinsic interest in technology and have some degree of technical aptitude beyond the average population. Thus, key technical terrain such as makerspaces, maker faires, code camps, and robotics competitions may make finding cyber talent more efficient and timely. To find cyber talent internal to the Army, DoD-sponsored venues such as permanent on-base maker labs would provide “prime hunting grounds” for cyber talent recruiters. To find cyber talent outside of the Army, commercial maker events and cyber contests, such as CyberPatriot, are inducements for civilian cyber talent.

FIX PIECE: Identify Cyber Talent and Recruit

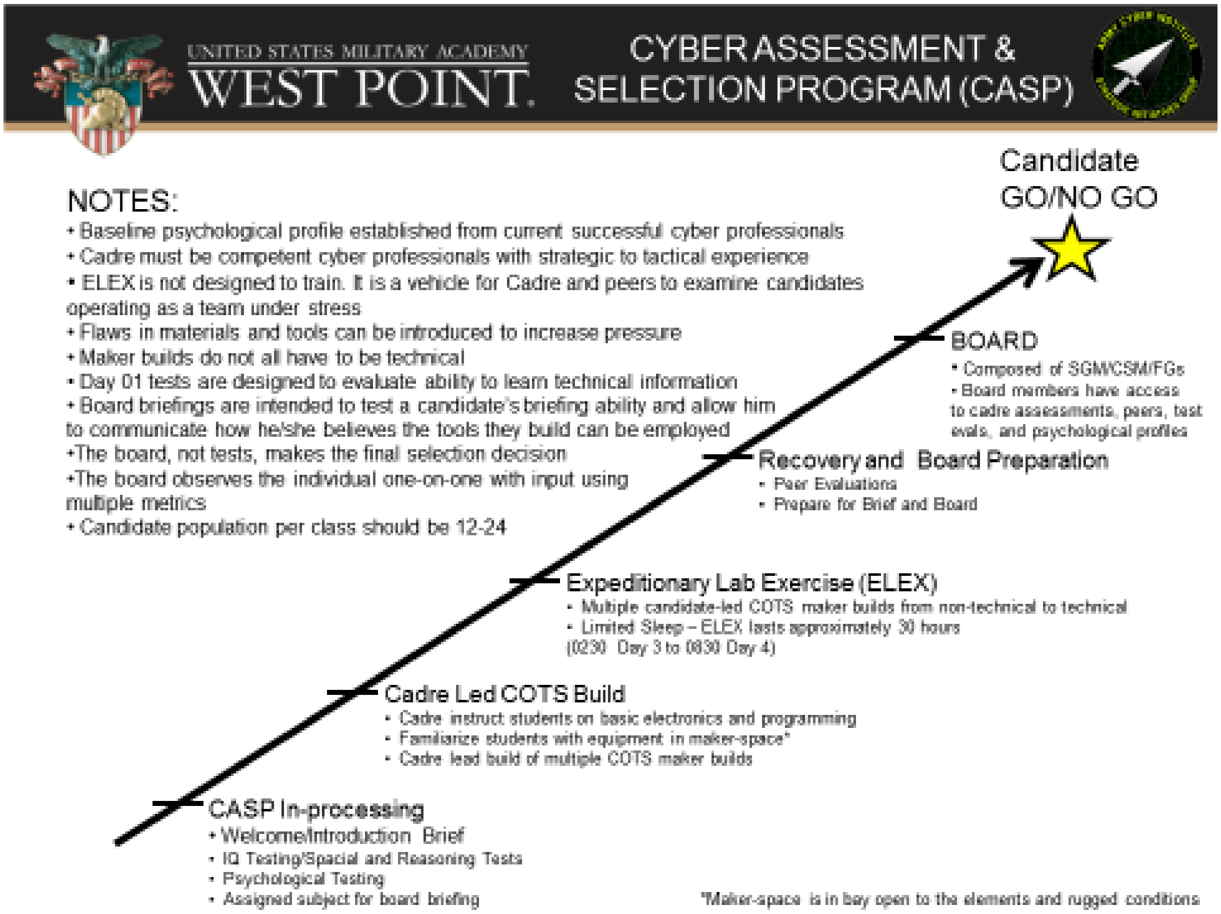
Once the key technical terrain is recognized, CTI recruiters must identify, track, and lastly engage cyber-talented individuals operating in the key technical terrain to recruit them as candidates to attend the Cyber Assessment and Selection Process (CASP). There is great value in fixing a combination of internal soldiers and external civilian talent at key technical terrain as it would provide a great deal of diversity to a technical field requiring agility, resilience, and adaptability given the uncertainty of the future operating environment and the velocity of technological change. This may require two permutations of CASP: one to accession Soldiers in non-cyber related MOSs and one to accession civilians or other population out of the joint and inter-agency community. This paper will focus solely on a CASP built for Soldiers.

FINISH PIECE: Cyber Assessment & Selection Program (CASP)

One proposed way to assess potential cyber personnel is to conduct a 5-day assessment course similar to one used by the 75th Ranger Regiment. Once identified and engaged during the “Find” and “Fix” pieces by recruiters at civilian and DoD key technical terrain, candidates would be invited to attend the CASP to gain entry into the Cyber branch. The Cyber Center of Excellence at Ft. Gordon could operate the program or at other Army cyber “centers of gravity.” CASP would consist of a one week program enabling both quantitative and qualitative assessments and should contain the following elements:

- Practical tests including reasoning, problem-solving and spatial awareness examinations
- Designing and building tools with components ranging from popsicle sticks to Commercial Off-The-Shelf (COTS) electronics and open-source software
- Mini- Capture The Flag (CTF) event or extended build tests
- Interview with a psychologist
- Interviews with cyber school cadre
- Culminating review board consisting of senior cyber officers, warrant officers, noncommissioned officers, course cadre, and a psychologist

The COTS build and/or a CTF exercise allows the cyber cadre to evaluate a candidate’s ability to work in an unknown and unfamiliar environment under stressful, sleep-deprived conditions. Throughout the course, cadre assesses each candidates’ creative abilities and ability to work as a team member and observe their resilience to stress and failure. A hands-on, qualitative evaluation is important to identify traits, knowledge and skills needed for cyber operations. Many of these skills and aptitudes will parallel those of cyberspace opponents, so testing candidates in a CTF environment against a red team, in a ‘cyber range’ is a must [15]. This testing could also help identify potential cyber leaders among the candidate population [5].



UNITED STATES MILITARY ACADEMY

WEST POINT.

CYBER ASSESSMENT & SELECTION PROGRAM (CASP)

NOTES:

- Baseline psychological profile established from current successful cyber professionals
- Cadre must be competent cyber professionals with strategic to tactical experience
- ELEX is not designed to train. It is a vehicle for Cadre and peers to examine candidates operating as a team under stress
- Flaws in materials and tools can be introduced to increase pressure
- Maker builds do not all have to be technical
- Day 01 tests are designed to evaluate ability to learn technical information
- Board briefings are intended to test a candidate's briefing ability and allow him to communicate how he/she believes the tools they build can be employed
- The board, not tests, makes the final selection decision
- The board observes the individual one-on-one with input using multiple metrics
- Candidate population per class should be 12-24

Candidate GO/NO GO

BOARD

- Composed of SGM/CSM/FGs
- Board members have access to cadre assessments, peers, test evals, and psychological profiles

Recovery and Board Preparation

- Peer Evaluations
- Prepare for Brief and Board

Expeditionary Lab Exercise (ELEX)

- Multiple candidate-led COTS maker builds from non-technical to technical
- Limited Sleep – ELEX lasts approximately 30 hours (0230 Day 3 to 0830 Day 4)

Cadre Led COTS Build

- Cadre instruct students on basic electronics and programming
- Familiarize students with equipment in maker-space*
- Cadre lead build of multiple COTS maker builds

CASP In-processing

- Welcome/Introduction Brief
- IQ Testing/Spacial and Reasoning Tests
- Psychological Testing
- Assigned subject for board briefing

*Maker-space is in bay open to the elements and rugged conditions

Figure 3. CASP Chart.

An essential component of the CASP is the interview with a cyber-psychologist. There is a pressing need to fill cyber positions throughout the force, but only with the right people. Not all personnel that review favorably quantitatively on paper will be a good fit in the cyber force. A final review board where the candidate reviews face-to-face by senior cyber leaders, course cadre, and psychologists is a critical gate each candidate must pass. The duty of the board members is to assess the quantitative and qualitative strengths and weaknesses of each candidate to determine whether they fit the criteria of a cyber professional. Cyber training provided by the military is modeled on the techniques, tactics and methodologies of attackers so defenders have the knowledge to defend friendly cyber operations [16-18]. The institution has the mission to identify the proper personnel and provide the environment and culture to create a successful cyber force [18].

Instrument Results

Over 51,000 military applicants took the CT/ICTL during the test phase [11], and analysis of the CT/ICTL data suggests it was a better predictor of Military Occupational Specialties 25B Information Technology Specialist and 25N Cyber Network Defender Advanced Individual Training success than existing ASVAB Armed Forces Qualification Test subtest scores, including the Electronics Information. These subtests are commonly used to select applicants for many of the cyber fields [10]. Data showed the CT/ICTL was a significant performance predictor in the Navy Cryptologic Technician (CTN) school for both grade point average and successful graduation status and was an improved predictor than the CTN selection composites in use during that time [10]. The Air Force began use of the CT/ICTL in June 2014. Their use of the test expanded the qualified applicant pool by including those that scored five percentile points below the existing general cutoff scores but scored high enough on the CT/ICTL to be considered for cyber training [11]. Data from Air Force testing using the CT/ICTL showed incremental validity in selecting for several Air Force cyber and non-cyber career fields [9].

Limited data about the CTE test results was provided to the CCoE, and the data shows some positive correlation between high CTE exam scores and high SANS GIAC Certified Incident Handler (GCIH) exam scores. The positive correlation exceeds the correlation between the ASVAB General Technical score and the GCIH exam score for the limited study groups. In the SANS-provided data, the CTE was a better indicator of success in SANS exams than standard ASVAB subtest scores. It is not clear if the SANS exams are a measure of cyber aptitude or cyber skills and knowledge [13].

The CATA is still in the early design phase with a predicted 25-month time frame before final delivery of the test [19]. CATA's goal to predict performance outcome of one more 'challenging' cyber courses, rather than performance in an initial-entry cyber course [20]. CASL notified the CCoE in June 2015 the Air Force CIO-A6/A6SF intended to fund the CATA work. The intent is to create an initial screening instrument used at the Military Entrance Processing Stations (MEPS) with the standard ASVAB [21]. See Table 3 for comparison between the three instruments.

Table 3. Comparison between test instruments

	Aptitude	Knowledge		Computer-based	In use	Fee-based
CATA	Y	N		UNK	N	N
CT+ASVAB	Y	Y		N	Y	N
CTE	UNK*	Y		Y	Y	Y

Discussion and Recommendations

The pool of potential candidates for the Army cyber force is two groups: new entrants into the military and those already serving in the Total Force. Each group needs a tailored talent assessment rather than a ‘universal’ fit. While a universal assessment would be the most efficient approach, such an assessment would lose effectiveness in identifying cyber talent. Assessments measure a specific population and as the population bounds increase, the less effective the assessment is in identifying a specific subgroup.

As noted in earlier sections, the ASVAB assesses new accessions into the military, a population that has lower-levels of knowledge and experience. The outcome expected for the test is to measure success in completing entry-level military training. The test is periodically ‘normed’ or baselined to changing demographics in the entry-level pool of the US population. The ASVAB is not designed for older, experienced populations, e.g. serving members of the military with several years of service and entrance-level military training, and would not be a good measuring instrument for such a population [22].

Evaluating transfers into the cyber force requires a different process. Rather than give existing informational assessments (i.e. ASVAB & CT/ICTL), an interview and testing process discussed in CASP would be the better choice in identifying cyber talent. The CASP would not be the choice for assessing new accessions as it would assess approximately 12-25 personnel in a week and has significant costs for this small scale example. These costs could be supported to increase the success of selecting the right cyber personnel from within the serving force but would probably be excessive if applied to all new accessions. An alternative to CASP-like evaluation for this population would be a population-independent cyber aptitude assessment instrument (e.g. the CATA) coupled with an interview process. An intensive interview process should be used in place of the CASP or CATA if they are not available. As noted in [18], “In information security education, we teach skills to our students that are potentially dangerous.”

Another issue facing the identification process is the pressure of time. Personnel identified in early 2016 and completing basic training in mid to late 2016 will start the first cyber training classes for new accessions in early 2017, This timeline mandates an assessment solution be available before Army Recruiting Command starts recruiting for new accessions to fill these cyber training classes.

The solutions immediately available are the ASVAB + CT test or the SANS CTE. The CTE, as a proprietary instrument, costs money for each time it is used and potentially costing incurring excessive costs. There are questions on what the CTE actually measures, as discussed in the previous section. The ASVAB + CT is available and, as the writing of this paper, currently being used by the Air Force to select their cyber personnel. Even with this success, the Air Force is working to provide a long-term solution that may provide a better instrument for identifying talent: the CATA.

The CATA stands out as the long-term solution for cyber assessment. The Air Force recently funded research with a 25-month timeline for deployment. Eventually, the Air Force plan is to use a combination of the ASVAB+CT and the CATA to identify cyber talent, with the instruments administered at MEPS. This combination may be the way forward, with the assumption the CATA can be proven to identify cyber aptitude.

Table 4 documents the recommendations for each population and for each timeline. If MEPS fields the ASVAB+CT, it would allow for identification of a potential pool of cyber personnel and provide a force-wide cyber assessment with scores recorded in permanent personnel records. The ASVAB+CT should continue as a screening function once the CATA is deployed, with the assumption the CATA would be administered to those that score high on the ASVAB+CT. The CASP should be the primary assessment for serving personnel assuming the costs could be supported.

Table 4. Recommendations for talent assessment by population

Population	**Short – Term**	**Long - Term**
New Accessions	ASVAB+CT	ASVAB+CT with CATA
Current Force	CASP or application/interview	CATA + CASP

References

[1] Joints Chief of Staff, "Joint Publication 3-12: Cyberspace Operations," 2013.

[2] Department of Defense, "Cyberspace workforce strategy," 2013.

[3] D. J. Kay, T. J. Pudas and B. Young. Preparing the pipeline: The US cyber workforce for the future. *Defense Horizons* [Online]. *(72),* 2012. Available: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA577318.

[4] C. Paul, I. R. Porche III and E. Axelband. The other quiet professionals: Lessons for future cyber forces from the evolution of special forces. RAND Corporation. Santa Monica, CA. 2014[Online]. Available: http://www.rand.org/pubs/research_reports/RR780.html.

[5] K. L. Alfonso. A cyber proving ground: The search for cyber genius. *Air & Space Power Journal* [Online]. pp. 61-66. 2010. Available: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA595976.

[6] S. G. Campbell, P. O'Rourke and M. F. Bunting, "Assessing aptitude for cybersecurity training: The cyber aptitude and talent assessment (CATA)," Nov., 2104.

[7] S. G. Campbell, P. O'Rourke, J. I. Harbison and M. F. Bunting, "Assessing Aptitude for cybersecurity training: the cyber aptitude and talent assessment, technical details," Dec., 2014.

[8] S. G. Campbell, P. O'Rourke and M. F. Bunting, "Identifying dimensions of cyber aptitude: the design of the cyber aptitude and talent assessment," 2015.

[9] T. E. Diaz, M. C. Reeder and D. M. Trippe, "Cyber test: Selection and classification," Human Resources Research Organization, Alexandria, VA, 2015.

[10] D. M. Trippe, M. C. Reeder, D. Brown, I. J. Jose, T. S. Heffner, A. P. Wind, K. G. Canali and K. I. Thomas, "Validation of the information/communications technology literacy (ICTL) test," US Army Research Institute, Washington, DC, 2015.

[11] D. M. Trippe, K. O. Moriarty, T. L. Russell, T. R. Carretta and A. S. Beatty. Development of a cyber/information technology knowledge test for military enlisted technical training qualification. *Mil. Psychol.* [Online]. *26(3),* pp. 182-198. 2014. Available: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA609376.

[12] T. L. Russell and W. S. Sellman, "Information and communication technology literacy test training school validation: Phase II final report," Human Resources Research Organization, Alexandria, VA, Tech. Rep. FR-09-89, 2010.

[13] SANS.org, "What is cybertalent enhanced (CTE)?" 2014.

[14] US Army, "Army techniques publication targeting," US Army, Washington, DC, Tech. Rep. 3-60, May. 2015.

[15] T. S. Smith. In pursuit of an aptitude test for potential cyberspace warriors. [Online]. pp. 1-103. 2007. Available: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA469300.

[16] G. Ledin Jr. The growing harm of not teaching malware. *Commun ACM 54(2),* pp. 32-34. 2011.

[17] S. Bratus, A. Shubina and M. E. Locasto. Teaching the principles of the hacker curriculum to undergraduates. Presented at Proceedings of the 41st ACM Technical Symposium on Computer Science Education. 2010, .

[18] T. Cook, G. Conti and D. Raymond. When good ninjas turn bad: Preventing your students from becoming the threat. Presented at Proceedings of the 16th Colloquium for Information System Security Education. 2012, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.448.535&rep=rep1&type=pdf.

[19] J. F. Cochran, "RE: Cyber aptitude assessment," 2015.

[20] S. G. Campbell, P. O'Rourke and M. F. Bunting, "Research design: validating cyber aptitude measures on learner populations," Dec., 2014.

[21] M. F. Bunting, "Update from CASL 8 June 2015," 08 Jun, 2015.

[22] D. O. Segall. Development and evaluation of the 1997 ASVAB score scale. *Innovations in Computerized Assessment* 2004.