Cyber Trust IQ

Assessing Aptitude. Creating Pathways. Precise Placement.

2016

Characterizing cybersecurity jobs: Applying the Cyber Aptitude and Talent Assessment Framework

Characterizing cybersecurity jobs: Applying the Cyber Aptitude and Talent Assessment Framework

Susan G. Campbell, Lelyn D. Saner, Michael F. Bunting
University of Maryland
7005 52nd Avenue
College Park, MD 20742
[scampbell, lsaner, mbunting]@casl.umd.edu

ABSTRACT
Characterizing what makes cybersecurity professions difficult involves several components, including specifying the cognitive and functional requirements for performing job-related tasks. Many frameworks that have been proposed are focused on functional requirements of cyber work roles, including the knowledge, skills, and abilities associated with them. In contrast, we have proposed a framework for classifying cybersecurity jobs according to the cognitive demands of each job and for matching applicants to jobs based on their aptitudes for key cognitive skills (e.g., responding to network activity in real-time). In this phase of research, we are investigating several cybersecurity jobs (such as operators vs. analysts), converting the high-level functional tasks of each job into elementary tasks, in order to determine what cognitive requirements distinguish the jobs. We will then examine how the models of cognitive demands by job can be used to inform the designs of aptitude tests for different kinds of jobs. In this poster, we will describe our framework in more detail and how it can be applied toward matching people with the jobs that fit them best.

CCS Concepts
• **Social and professional topics~ Computer and information systems training** • *Social and professional topics~ Computational thinking* • Social and professional topics~ Student assessment • Applied computing~ Cyberwarfare

Keywords
Aptitude testing; job analysis; task analysis; cybersecurity workforce; selection.

1. INTRODUCTION
One of the challenges in cybersecurity is selecting the right people. The problems are manifold: not only is it difficult to assess existing skills and abilities, but future challenges may require different skills and abilities. Organizations must find ways to increase the number of people they select while simultaneously improving their selection practices. One approach to addressing this problem is to assess aptitude in addition to current skills. The problem with assessing aptitude is characterizing what cognitive characteristics successful cybersecurity professionals must possess.

HotSoS '16, April 19-21, 2016, Pittsburgh, PA, USA
ACM 978-1-4503-4277-3/16/04.
http://dx.doi.org/10.1145/2898375.2898394

Cybersecurity occupations have a function in common: they exist to maintain and protect computer networks. These occupations, however, do not necessarily involve the same technical skills, cognitive abilities, or temperamental characteristics. For instance, the job of an interactive operator is not the same as the job of a developer, and the job of an analyst is not the same as the job of a network architect. Required knowledge may overlap between the jobs and fall into the same broad categories, but the skills and tools are different. In this paper, we will describe how we plan to characterize jobs in terms of their cognitive requirements as a complement to other efforts to characterize the cybersecurity workforce.

Previous work in characterizing cyber occupations has resulted in resources like the National Initiative for Cyber Education (NICE) workforce framework. The NICE framework describes the jobs that contribute to a successful cybersecurity posture in terms of their functional requirements, but it does not characterize the cognitive requirements.

In order to create selection instruments to predict who can do these jobs, we must first characterize the jobs and the people who do them well. Our team has created the Cyber Aptitude and Talent Assessment (CATA) framework, which aims to provide categories that can be used to assess the cognitive requirements of particular jobs. Our current research aim is to characterize a small set of jobs and to determine whether the framework provides us with useful information to create an aptitude test that can select people not just for cybersecurity jobs in general, but for those jobs specifically.

1.1 State of the art
The current best practice for selecting cybersecurity personnel varies by position and type of organization. In general, however, the best selection systems look for some combination of credentials, knowledge, and skills. For private-sector and civilian government employees, hiring managers may look for commercial certifications and academic credentials.

For military personnel, selection systems generally differ for officers and enlisted personnel. As an example, the US Navy requires applicants for Cyber Warfare Engineer positions to possess a Computer Science or Computer Engineering bachelor's degree from a particular list of institutions [4]. For enlisted personnel, the requirement for a Cryptologic Technician Networks job is a high school diploma and scores higher than a certain cutoff on the Armed Services Vocational Aptitude Battery (ASVAB). In addition, the United States Air Force has developed an Information/Communications Technology Literacy (ICTL) test, which assesses basic cyber knowledge in recruits [3].

These credentials and tests are a good measure of what a potential hire can currently do, but they do not necessarily tap into

potential, especially in people who do not yet have some level of skill. Unfortunately, due to cybersecurity being a relatively new field, there are many adults who have not had an opportunity to formally study cybersecurity, but who may be able to do cybersecurity jobs if given the appropriate training. Therefore, tests of more general cognitive abilities and aptitudes can add to the assessment of credentials and knowledge to broaden the pool of potential hires.

1.2 Goals of this research

We intend to use the outcomes of this research to propose aptitude tests to augment existing credential-based and knowledge-based selection systems, but the focus of this paper is on exploring the research methods used to investigate the jobs themselves and link those job demands to aptitude test components.

2. The CATA framework

The CATA framework [1] is one way of characterizing jobs and candidates in order to determine the best match between the cognitive and temperamental demands of a particular job and the strengths of a particular candidate. The framework distinguishes between general cognitive abilities, which apply across cybersecurity jobs and beyond cybersecurity jobs, and job-specific abilities, which depend on the characteristics of a specific job on a pair of dimensions, as shown in Figure 1

The two dimensions of the diagram are real-time/exhaustive and initiating/responding. Real-time action requires the ability to act quickly and accurately without becoming distracted, while exhaustive action requires the ability to consider all possibilities without prematurely jumping to conclusions. Initiating actions requires hypothesizing about the potential outcomes of actions and generating creative solutions to problems, while responsive actions require vigilance and an ability to detect anomalies in the environment.

Orthogonally, actions can also vary on being more and less cognitively complex. The general trend, however, is for less cognitively complex job tasks to be automated as much as possible, so it does not seem advantageous to try to identify people who can perform tasks that are not cognitively complex.

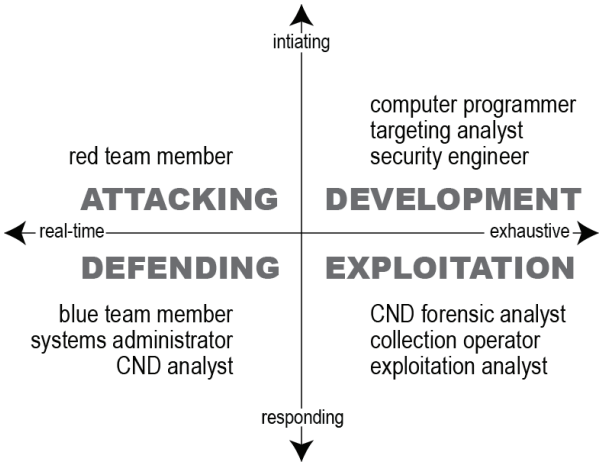

Figure 1. CATA framework diagram. Jobs and tasks can be categorized along each dimension. The named quadrants correspond to a major, characteristic category of tasks that would fit the listed dimensions, while the jobs titles listed are samples from the NICE workforce framework.

3. Situating tasks within the framework

The tasks that make up a job can be rated along the dimensions of the CATA framework, but that rating is not straightforward. One of the challenges of fitting tasks to the CATA framework is determining what constitutes a task. Traditional job analyses include lists of tasks that employees are expected to perform along with lists of knowledge, skills, and abilities (KSAs) needed to be able to perform them.

As an example, the NICE framework provides a list of tasks for the "Software Assurance and Security Engineering" specialty area, and this list includes tasks like, "prepare detailed workflow charts and diagrams that describe input, output, and logical operation, and convert them into a series of instructions coded in a computer language" [2].

The main challenge of this work, therefore, is to convert the high-level tasks as listed in the NICE framework into atomic tasks that can be rated on our framework of cognitive demands

Table 1. Example of task ratings for hypothetical tasks on a scale where -10 represents a completely real-time task, while 10 represents a completely exhaustive task. Similarly, -10 represents a task that requires only responding, while 10 represents a task that is entirely initiating.

Task	Complexity [0, 10]	Real-time ⇔ Exhaustive [-10, 10]	Responding ⇔ Initiating [-10, 10]
Write countermeasures to counteract potential attacks	9	5	2
Recognize novel intrusion	8	-10	-10
Respond to intrusion by activating existing countermeasures	5	-10	-8

4. Building jobs from sets of tasks

The tasks that we propose to rate, however, are not equally important to all jobs. Some tasks are common across all jobs, and therefore those tasks will not distinguish among jobs. Other tasks are not performed in a particular job at all. As shown in Table 2, we propose to ask subject-matter experts to rate each task on how important it is to a particular work role.

One way to categorize a job, therefore, would be to plot each task on a grid to see which quadrant(s) the tasks primarily fall into, as shown in Figure 2. In this case, the tasks primarily involve initiating events and exhaustive processing; these tasks are not performed in response to any immediately pressing situation and it would generally be more important that they be completed correctly than that they be completed especially quickly.

Table 2. Example of importance ratings for particular tasks within particular jobs.

Task	Operator importance [0, 10]	Developer importance [0, 10]
Write countermeasures to counteract potential attacks	0	10
Recognize novel intrusion	9	1
Respond to intrusion by activating existing countermeasures	10	0

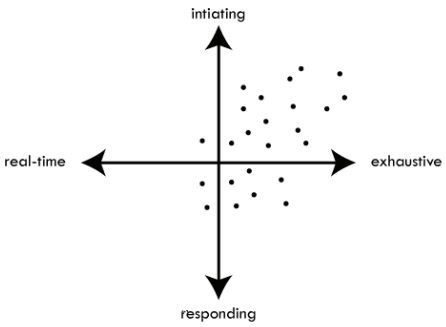

Figure 2. Plot of hypothetical job on quadrant diagram. The plotted locations correspond to coordinates based on the ratings provided in Table 1.

The next step would then be to have subject-matter experts or expert job incumbents rate the importance of each task for a job, leading to a more precise importance polygon. The output of this process, then, would be a set of tasks, located on the quadrant model, with a set of importance ratings. Such sets could then be matched to the aptitude profiles of particular job applicants to determine what job would best fit their aptitude.

5. Building tests and aptitude profiles

The general goal of an aptitude test for a particular job is to determine who is ready to learn the necessary skills. As noted above, however, not all cybersecurity skills are required for all cybersecurity jobs, which implies that a good set of aptitude tests would be able to target specific jobs.

We are designing test batteries based on the CATA framework to include assessments for the quadrants that are relevant for a particular job as well as assessments of critical thinking, which will predict the ability to learn the material.

The CATA framework would not be used the same way for individuals that it is used for tasks; a person could be good at any of the abilities necessary to perform particular jobs, or none of them. Someone could be good both at real-time action when necessary and exhaustive action when necessary. We suggest the diagram shown in Figure 3 as a potential way to think about a person's aptitude, with ratings for each construct evaluated separately, including cyber knowledge and critical thinking. As suggested in that figure, a person could be good at both initiating and responding, and therefore might be almost equally good at both developer and analyst/forensics roles.

In order to validate test batteries based on the CATA framework, we intend to determine if the test components we have linked to particular quadrants predict performance on tasks that we have identified as belonging to those quadrants. We have planned several validation tests, some for general ability to acquire cybersecurity knowledge and others to see if the framework can distinguish among jobs that we hypothesize to belong to different quadrants.

6. Conclusions and future work

We have developed these methods to create aptitude tests for military and civilian selection. By characterizing the cognitive demands of each job, we propose to link the tests to work roles and improve assignment of cyber personnel to jobs they have the potential to excel at.

Once we have completed this analysis, we can ask a few additional questions about our proposed framework, like whether there are additional dimensions that have emerged from breaking the tasks down into atomic components, or whether there are job-specific tasks that are essential but that are not captured by our framework. Future iterations could refine the coding scheme to match aptitude profiles more closely to job demands, providing metric information instead of qualitative classifications.

Looking even further ahead, we would eventually like to be able to automate some of the profile generation or job characterization. For situations where mission readiness can be defined precisely, for instance, required aptitudes could eventually be generated directly from the mission ready checklist for specific work roles.

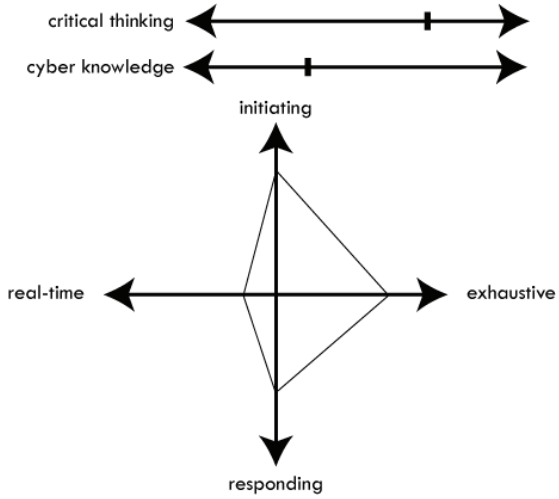

Figure 3. Sample aptitude profile showing someone with a low level of knowledge, but a high level of critical thinking ability and a strength in the developer quadrant and the analyst quadrant.

7. REFERENCES

[1] Campbell, S.G., O'Rourke, P., & Bunting, M.F. (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*, 721-725. doi:10.1177/1541931215591170

[2] National Initiative for Cybersecurity Education (2014). *DRAFT National Cybersecurity Workforce Framework Version 2.0.*

[3] Trippe, D.M., Moriarty, K.O., Russell, T.L., Carretta, T.R., & Beatty, A.S. (2014). Development of a cyber/information technology knowledge test for military enlisted technical training qualification. *Military Psychology* 26(3), 182-198. doi:10.1037/mil0000042

[4] United States Navy Recruiting Command (2016). Become a Naval Cyber Warfare Engineer. http://www.navy.com/careers/information-and-technology/cyber-warfare-engineer.html#ft-qualifications-&-requirements retrieved 2016-01-27.

Cyber Trust IQ

Assessing Aptitude. Creating Pathways. Precise Placement.

Characterizing cybersecurity jobs: Applying the Cyber Aptitude and Talent Assessment Framework

CONTACT

A: Research Triangle Park North Carolina
E: info@cyber-alliance.com
T: (984) 293-7628