What shape peg are you? Different cyber jobs require different cognitive skills

Susan G. Campbell
Center for Advanced Study of Language
University of Maryland
College Park, MD 20742
susanc@umd.edu

Petra Bradley
Center for Advanced Study of Language
University of Maryland
College Park, MD 20742
pbradley@casl.umd.edu

ABSTRACT

Though cyber workforce estimates generally collapse cyber workers into a single category, the job demands of work roles within cyber differ. We have built a model of what cognitive and dispositional characteristics are necessary for different categories of work roles within the cyber workforce. As part of testing that model, we interviewed workers in three divergent work roles within a large cyber organization. The organization asked us to investigate these work roles because they are difficult to fill, requiring a specific and specialized skill set. We found that the work roles did diverge in the types of cognitive abilities and training required, though they did not necessarily fit in the locations we had predicted within our model.

1. INTRODUCTION

The National Institute for Cybersecurity Education (NICE) has built a framework, called the NCWF (NICE Cybersecurity Workforce Framework) [3], which classifies 52 cyber work roles into seven categories, and further into 33 specialty areas. Each work role is characterized with the tasks that people within it perform and the knowledge, skills, and abilities (KSAs) that are required to successfully perform those tasks. The specialty areas and categories are defined by the functions that people within them perform for an organization, such as securely provisioning a network or analyzing information. This functional classification is useful for building a plan to recruit a workforce, but the function requirements may not completely determine the cognitive abilities that are required for jobs; work roles in different categories may be more cognitively similar to a targeted work role than work roles that share a category with it.

The Cyber Aptitude and Talent Assessment (CATA) framework [1] classifies jobs within cyber according only to their cognitive demands (as shown in Figure 1). The framework divides jobs and the tasks within them along two axes: initiating/responding and real-time/exhaustive. Jobs that require initiating actions involve planning and hypothesizing outcomes, while jobs that require responding involve vigilance and the ability to notice anomalies. Orthogonal to that distinction is the division between jobs that require quick decision-making (though not necessarily raw speed) and those that require the consideration of all options. The model allows the placement of jobs within quadrants, but the people who do particular jobs may have cognitive skills in all quadrants.

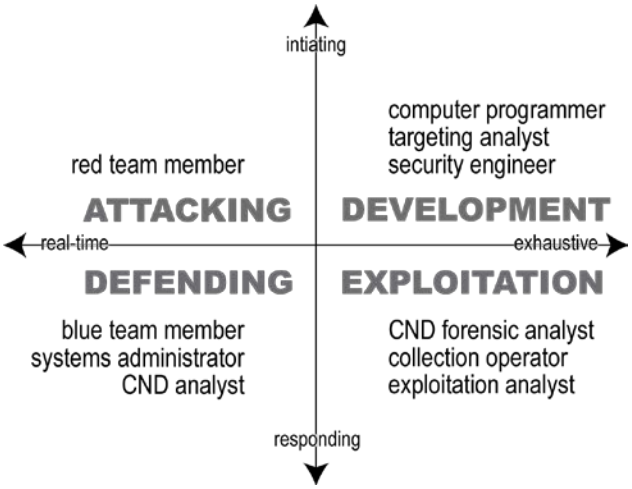

Figure 1. CATA framework quadrants illustrated with sample jobs from the NCWF.

In previous work, we have suggested that classifying jobs could be done by enumerating the tasks that people in a work role needed to perform and then rating the tasks on the dimensions of the model in order to, essentially, graph the job functions [2]. This approach assumes that the tasks that are performed by each person in the job are essentially the same, that individuals use the same cognitive abilities and skills to perform the tasks, and that we can represent the tasks in a way that is sufficiently precise to determine the cognitive demands of each task. The purpose of the study described in this paper was to determine whether the work roles under consideration were properly situated within the model.

As the name suggests, the CATA framework was initially designed to facilitate the development of aptitude tests for jobs that fit into different quadrants cognitively. For example, a

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018. August 12 -- 14, 2018, Baltimore, MD, USA.

developer may not need to be evaluated on their speed, and an analyst may not need to be evaluated on their creativity.

This investigation was part of an effort to build an aptitude test for assigning people to jobs within the organization we were studying. Instead of creating a test battery to fit a specific quadrant, the organization wanted to build a general aptitude test that would allow them to assign personnel to jobs that fit their cognitive strengths.

In this study, we investigated the cognitive demands of three targeted work roles within a large cyber organization using a semi-structured interview approach. Based on the results of these interviews, we customized a prototype aptitude battery and administered it to people in different work roles within the target organization. An overview of those results was presented at the 2017 NICE Conference and Expo [4].

The three work roles were identified by the organization as cognitively demanding and requiring specialized training that students described as "very challenging." Two of them, exploitation analyst (EA) and cyber operator (CO), corresponded with work roles in the NCWF (EA: AN-EXP-001; CO: CO-OPS-001), but the third did not. This third role was tool development (TD), which involves building tools to enable operations and analysis.

We predicted that TDs would fit into the "development" quadrant, as shown in Figure 2, while EAs would fit into the "exploitation" quadrant, and COs would fit into either the "attacking" or "defending" quadrants.

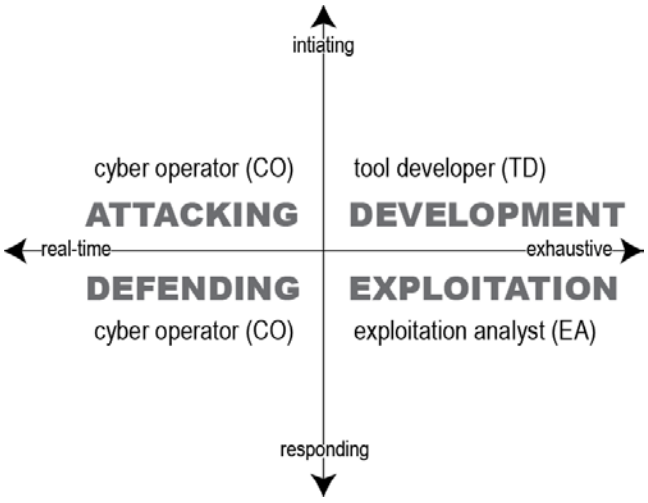

Figure 2. Hypothesized location of work roles of interest to current study in CATA framework.

2. METHODS

First, we reviewed the existing documentation on each work role that the cyber organization was interested in characterizing.

The organization then provided us with contact information for a subset of people who were successfully performing each work role, and we recruited a small number of individuals in each of the work roles for cognitive task analysis interviews (CO *n*=9, EA *n*=9, TD *n*=8). Each interviewee answered the same questions, and the semi-structured interview allowed us to ask follow-up questions as appropriate.

The interview protocol comprised 42 questions, organized into 5 sections: demographics, job requirements, KSAs, standards and metrics, and past experience. Some sample questions included:

- For how many years have you been doing cybersecurity work?
- Please describe your typical workday.
- Please describe 3-4 tasks that you think are most critical for, or that best define, your job.
- How often do you perform each of the tasks you've described in a typical week? (several times per day, once per day, several times per week, once a week, never)
- On a scale of 1-5, with 1 being the least challenging and 5 being the most challenging, how challenging is each task you have just described overall?
- On a scale of 1-5, with 1 being the least satisfying and 5 being the most satisfying, how satisfying is each task you have described overall?
- Are there any dependencies between these tasks? Are any of them subtasks of others or do they generally need to be done in a particular sequence?
- Does your job involve time constraints such as deadlines, precision timing, or situations to which you must respond in real time? If so, please describe.
- Does your job require you to maintain a mental picture of how elements or entities are distributed and/or interrelated?
- How often do you need to adapt your work practices to new scenarios or contexts? (several times per day, once per day, several times per week, once a week, never)
- Which skills that you currently have do you believe are most critical for doing your job?
- What other types of past work experience have you had, if any, that you believe helped to prepare you for this job?

We coded the answers to correspond with the axes of the CATA framework and to identify emergent trends among interviewees.

3. RESULTS

The work role tasks described by participants roughly corresponded to the descriptions provided in the organization documentation and in the NCWF. In general, TDs reported that the tasks that defined their job related to implementing (7 of 8 interviewees) and debugging (8 of 8 interviewees) software, while EAs reported planning (10 of 10 interviewees) and analyzing (10 of 10 interviewees) operations, and COs reported executing (7 of 9 interviewees) operations.

We found that workers' conception of their jobs varied from person to person within the same work role and in the same organization, however. At least one person in each of the three work roles mentioned communications, customer relations, professional development, operational planning, or operational analysis as a central task. In general, the interview answers supported the idea that the specific cognitive demands of these three jobs differ, but that there are common tasks.

Unfortunately, detailed descriptions of the tasks most critical to each job are considered proprietary. However, we can share information about how the cognitive aspects of the reported tasks allowed us to situate the work roles within the CATA framework and which KSAs the participants found necessary for each work role.

3.1 Placement into Quadrants

We found that the placement of the jobs within the CATA model did not match our predictions exactly.

TDs did report that their jobs tended not to involve real-time work, as predicted, while COs reported that their jobs mostly involved real-time work, also as predicted. However, EAs reported both real-time and exhaustive tasks, roughly corresponding to execution of plans (real-time) and making plans (exhaustive).

Some EAs and COs reported that anomaly detection and vigilance, which we included in the responsive category, were part of their jobs, while no TDs reported a need for either skill.

3.2 KSAs

As expected, TDs reported requiring knowledge of programming, while EAs and COs reported primarily requiring knowledge of networks and network concepts.

While participants reported on the knowledge requirements for their position, most of the interviewees had more difficulty reporting the skills and abilities required for their jobs when asked to list KSAs. This suggests either that we did not prime them enough to consider these cognitive capabilities, or that they do not introspect about the cognitive skills and abilities required to do their jobs. In a traditional cognitive task analysis this shortcoming could have been overcome with observations of individuals on the job. However, due to work place constraints, researchers were not permitted to observe cyber work.

Although the questions about KSAs yielded relatively scarce information about skills and abilities, some of the more-specific questions about job tasks revealed necessary skills and abilities. Interviewees in all three work roles reported attention to detail and mental imagery being important for correctly executing their work. They also reported that they needed to adapt to new situations on at least a weekly basis, with COs reporting that they needed to adapt to new situations daily.

3.3 Other Results

EAs and COs reported working in cross-functional teams and collaborating, while TDs mostly reported working with other TDs and did not report collaborating. This might imply EAs and COs have a greater need for understanding others' work in order to collaborate. Future work might examine the cognitive skills necessary for successful collaboration across work roles.

4. CONCLUSIONS

These results are limited by the small sample size and participants' difficulty in enumerating skills and abilities required for their jobs, but they suggest that characterizing specific jobs within the cyber workforce by knowledge and cognitive skill requirements in addition to their functional requirements could improve targeted recruitment, especially for high-level jobs requiring deep knowledge and complex cognitive skills.

5. FUTURE WORK

We followed this interview-based qualitative analysis with a study in which we tested people in these work roles on aptitude measures developed as part of the CATA project. Performance on the CATA subtests did not fully corroborate the interview findings, but, like the qualitative analysis, did show a basis for differentiating among the work roles. This finding is not unexpected, considering that individuals may have cognitive skills that exceed the requirements of their job. The lack of differentiation shown in cognitive ability measures underscores the need for investigation of the jobs as well as of the individuals that perform them.

Though the initial work supported the CATA framework predictions to some extent, future work will be needed to determine whether the model is appropriate for choosing aptitude measures. Future work should also be supplemented with cognitive task analysis measures that include observation of participants in the work role coded by cognitive psychologists who are trained to recognize the skills needed for and implemented during specific tasks.

6. ACKNOWLEDGMENTS

Dr. Lelyn Saner served as Principal Investigator for the research described in this presentation, and interviews and analyses were conducted by Dr. Susannah Paletz, Dr. Erica Michael, Dr. Polly O'Rourke, and Nicholas Pandža in addition to the authors.

This material is based upon work supported, in whole or in part, with funding from the United States Government. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the University of Maryland, College Park and/or any agency or entity of the United States Government. This material is being made available for personal or academic research use. If the intention is to use it for commercial reasons, please contact

University of Maryland's Office of Technology Commercialization at otc@umd.edu or (301) 405-3947.

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. *Human Factors and Ergonomics Society Annual Meeting Proceedings*, 721-725. doi:10.1177/1541931215591170

[2] Campbell, S.G., Saner, L.D., & Bunting, M.F. (2016). Characterizing cybersecurity jobs: Applying the Cyber Aptitude and Talent Assessment framework. *HotSoS '16*, 25-27. doi: 10.1145/2898375.2898394

[3] National Initiative for Cybersecurity Education (2017). *NICE Cybersecurity Workforce Framework*.

[4] Saner, L.D., Bradley, P., Michael, E., Pandža, N., & Campbell, S.G. (2017, November). The right one for the job: Using aptitude assessment to facilitate cybersecurity career decisions. *NICE Conference and Expo*, November 8, 2017, Dayton, OH.