Cyber Trust IQ

Assessing Aptitude. Creating Pathways. Precise Placement.

2016

Assessing Aptitude and Talent for Cyber Operations

Assessing Aptitude and Talent for Cyber Operations

Lelyn D. Saner[1], Susan Campbell[1], Petra Bradley[1], Erica Michael[1], Nicholas Pandza[1], and Michael Bunting[1],

[1] University of Maryland Center for Advanced Study of Language (UMD-CASL), College Park, MD, USA
{lsaner, scampbell, pbradley, emichael, npandza, mbunting}@casl.umd.edu

Abstract. In a world of rapidly evolving technology, it is an increasingly complex task to protect the integrity of information and security of infrastructural systems. Doing so demands a skilled workforce, which can only be assured with careful testing and selection of cyber operations specialists. We are conducting research to develop a cyber aptitude testing battery to improve selection and placement processes, but one of the biggest challenges lies in concisely characterizing the space of work roles. In this paper, we review some prior approaches to defining cyber work roles and describe our current approach to doing so at a more detailed level.

Keywords: Cybersecurity · Human Performance · Aptitude · Work Role Modeling

1 Introduction

The World Wide Web (WWW) connects people throughout the world, allowing for instantaneous communications and sharing of information across geographical and cultural boundaries. For all of the advantages that this technology affords, a number of major cyber security breaches in the last several years have raised general awareness of the risks associated with it as well. As technology continues to evolve, and more data and systems become integrated across networks, it becomes a more complex task to protect the integrity of information and the security of infrastructural systems. Furthermore, people share increasing amounts of personal information over social networking websites, such that maintaining privacy becomes more challenging.

These trends have increased the demand for a workforce of experts skilled at managing threats to information security. Although general training can bring many people up to a nominal level of expertise, people differ in their natural ability to acquire different skills. As such, given the rapidity with which change occurs in technology, and the diversity of factors that contribute to each cyber security breach, it is important to be able to identify at early stages those who are likely to be most successful at detecting events and responding to them quickly and creatively.

We are conducting research toward developing an instrument to assess individual aptitude for cyber security operations. Building on prior work done on assessment of

aptitude for foreign language acquisition, we plan to model the cyber aptitude test on similar instruments developed for measuring language aptitude. Both the language and the cyber aptitude tests are focused on cognitive abilities as the key component, however both are also designed to address several individual factors related to motivation and personality. It is also important to distinguish two separate goals of this work – to first design and develop a battery of aptitude tests that is predictive of successful performance in cyber operations work and to, second, use one or more versions that battery to differentially select people for particular cyber work roles based on their individual aptitude profiles.

Characterizing Cyber Work Roles. Perhaps the biggest challenge in testing aptitude for cyber is to isolate a concise characterization of what jobs and tasks fall within its field. Cyber operations require expertise in a number of mostly technical areas, such that it can be associated with and may draw operators from several disciplines, including computer science, engineering, and mathematics. More complicating is the fact that cyber operations are not limited to activity on computer networks. People live and act in both virtual spaces and in the real world, such that comprehensive cybersecurity requires an understanding of human motivation and behavior on top of network activity. Events occurring in both spaces need to be monitored because those occurring in one space can have significant effects in the other (e.g., malicious code infecting a power grid control system might deprive many people of electricity for some time).

A number of efforts have already been made to taxonomize the various work roles in the field of cyber operations. One of the most notable is the National Initiative for Cyber Education (NICE) framework, sponsored by the National Institutes for Standards and Technology (NIST), which identifies a set of generally defining tasks for work roles in 31 cybersecurity specialty areas, as well as the knowledge, skills, and abilities (KSAs) that are required to perform them [1]. The specialty areas themselves are grouped into seven categories: *securely provision, operate and maintain, protect and defend, investigate, collect and operate, analyze, and oversight and development*. Furthermore, although the framework identifies example work role titles for each specialty area, those lists are not exhaustive.

Other agencies and organizations have developed their own frameworks of cyber work roles, such as the Department of Homeland Security's (DHS's) list of 10 mission critical jobs [2]. As in the NICE framework, the tasks associated with each job are identified, and also included with each job is an analysis of the potential consequences if that job is not performed.

In both frameworks, however, the key drawback of the analysis for our purposes is that tasks are specified at too high of a level to reliably map the steps of task onto cognitive processes. For example, although the task, "*Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources*" ([1], p. 71) is clearly descriptive of the high-level goal of that activity, it does not specify the steps involved in accomplishing that goal or the cognitive demands that may be associated with performing them. In order to capture that, it is first necessary to establish a schema for the core cognitive dimensions of cyber work roles that can be used to represent them on that level of description. Then, with that in place, it is necessary to conduct an empirical task analysis, gathering descriptions of the work

roles from those who actually do them, and mapping those onto the cognitive schema [3, 4].

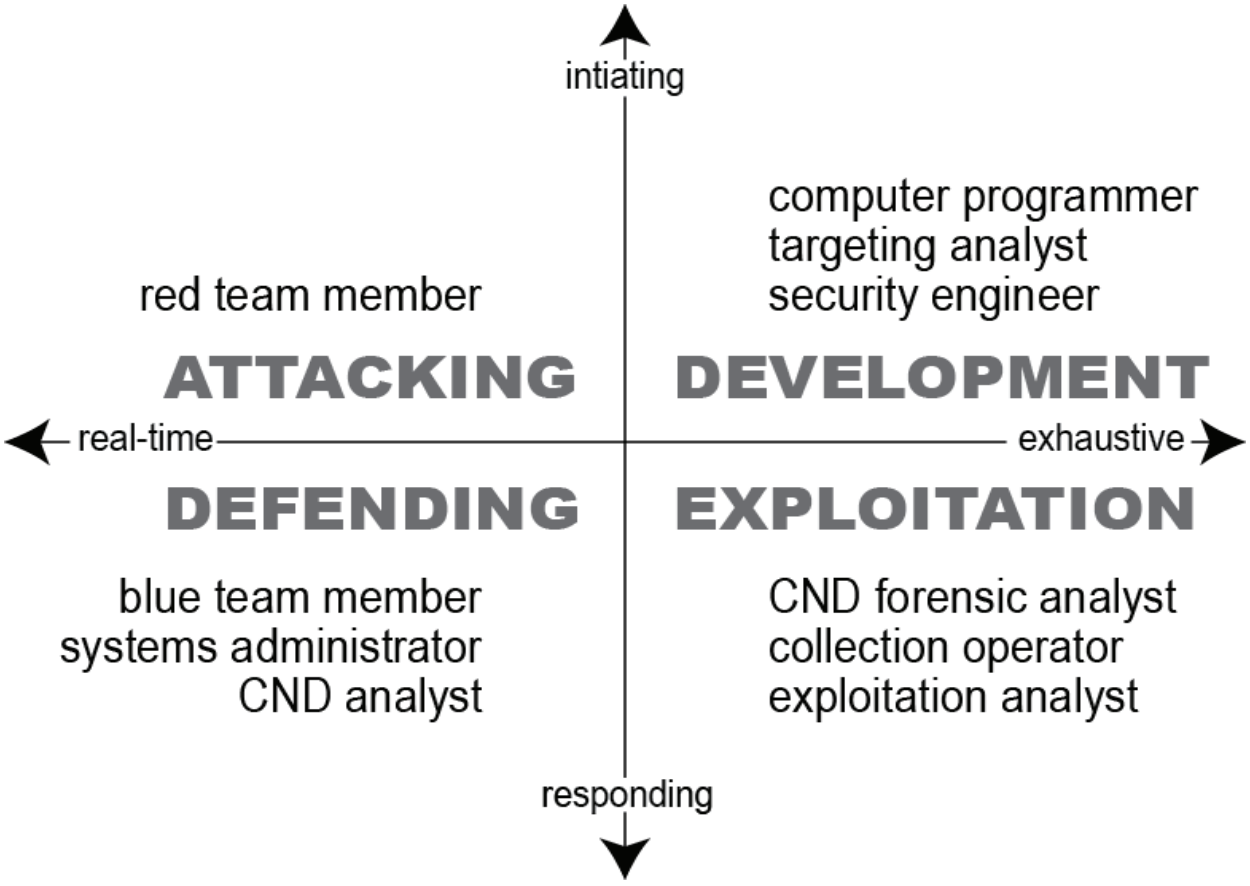

Fig. 1. Diagram of CATA framework, with sample work roles from the NICE framework as they might be categorized along each dimension.

Cognitive Dimensions of Cyber Work in Relation to Aptitude Test Development. Human cognition involves a range of processes including perception, attention, working memory, linguistic and conceptual processing of information, communication, long-term memory storage, judgment, decision-making, and problem solving. Task descriptions like the one cited above often suggest some of the cognitive processes involved. For example, "identify anomalous activity" suggests high attention and perception demands and although "identify potential threats" could be as simple as recognizing or recalling one of several types of threats stored from experience, it could require original processing of the current situation's unique details to reach a judgment about threat level and to generate a new threat category. However, these possibilities need to be supported by consulting with those who have experience doing the tasks regularly. The general cognitive processes just described are expected to differ across tasks, in terms of the roles they play and in what combination, and in so doing, they differentiate cyber tasks in terms of cognitive *complexity*. None of them are task-specific, however, since they apply across and beyond cyber operations work roles, so we still need dimensions that are targeted to cyber operations.

To this end, our team generated the Cyber Aptitude and Talent Assessment (CATA) framework [5], which utilizes two broader dimensions of cognitive demand

to situate cyber work roles in relation to each other (See Figure 1). The horizontal axis marks the range between operations that need to be conducted in *real-time* and those for which a complete and fully thought-out (i.e., *exhaustive*) strategy takes priority over time considerations. The vertical axis represents the continuum between *initiating* actions and *responding* to the actions of others.

When crossed, these dimensions create four quadrants that roughly correspond to four key classes of cyber network operations (CNO). *Attack* and *defend* operations are both on the real-time end of the spectrum; each clearly corresponding to the opposing poles of *initiating* and *responding*, respectively. In contrast, both *development* and *exploitation* operations generally require more planning and deliberation, such that they are both *exhaustive* endeavors despite being on different positions in the exchange cycle. Thus, granting that the boundaries between them on these dimensions may be fuzzy, work roles can be distinguished by larger operational goals that their component tasks support and by the complexity of tasks with respect to general cognitive abilities. This is illustrated in Figure 2, where each point represents a single task within a work role, and its coordinate position is based on its value on each of the dimensions.

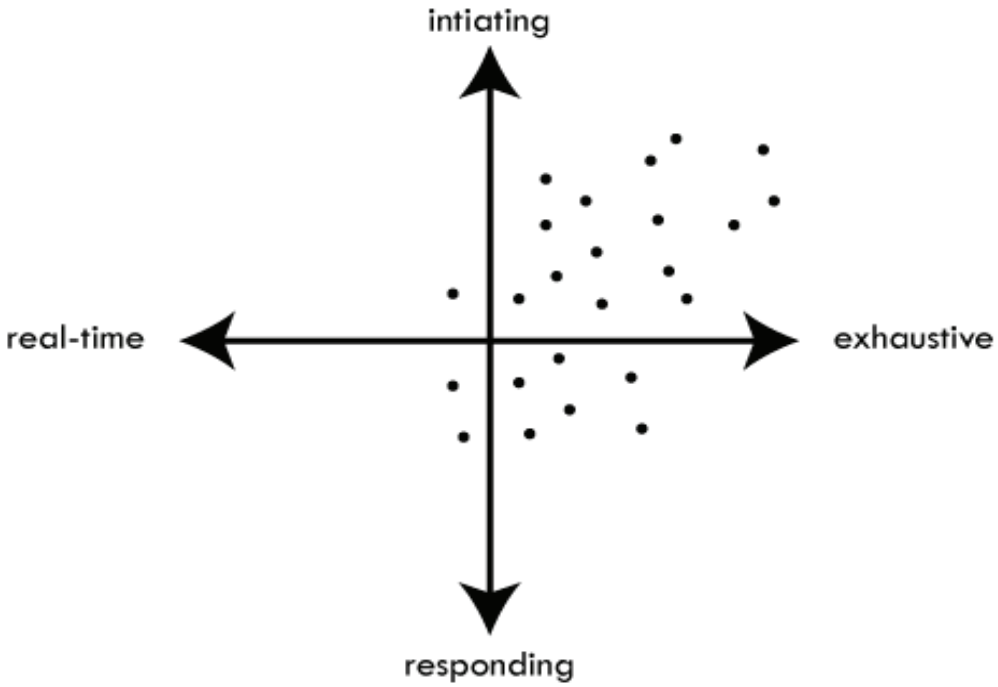

Fig. 2. Distribution of tasks on the quadrant model for a hypothetical work role, where position coordinates are based on ratings of tasks on each dimension.

Two other example tasks from the NICE framework, both within the *securely provision* specialty area, illustrate how the dimension values can diverge to put each task in a different quadrant (see Table 1). The values in the table here are hypothetical, and judgments about what values a task should have on each dimension cannot be made effectively based on the high level of description available in the framework. Therefore, we developed a questionnaire for people in cyber work roles with which to gather more details about their work tasks.

Table 1. Hypothetical values on dimensions for two example tasks from the NICE framework.

Task	Complexity [0, 10]	Real-time ←→ Exhaustive [-10, 10]	Responding/ ←→ Initiating [-10, 10]
Develop methods to monitor and measure risk, compliance, and assurance efforts	8	7	5
Inspect continuous monitoring results to confirm that the level of risk is within acceptable limits for the software application, network, or System	3	-8	-4

2 Methods

The questionnaire is administered as an in-person interview and is not specific to any one work role. It is designed to capture the features of the tasks that define a work role, the skills needed to be successful in that role, and the cognitive demands associated with it. There are 43 questions, some of which are focused on the task-level and some on the job-level, as well as several general background questions about experience (see Table 2 for examples).

Table 2. Categories of interview questions with examples.

Question Type	Examples
Background	What is your job title? How long have you been in your current position?
Work Tasks	Describe your typical workday. What is the most challenging aspect of each task?
Cognitive Demands of Job	Does your job involve time constraints? How routine is your work?
Knowledge, Skills, and Abilities (KSAs)	Which skills that you currently have are most critical for doing your job? What knowledge have you used the most?
Standards and Metrics	Are there clear expectations for what you should be accomplishing?

After responding to the background questions, participants are asked to describe their typical workday in their own words. The interviewer and note-taker verify that three to four tasks mentioned in the response are actually defining of the work role, and then ask the task-specific questions for each of them. The questions about cognitive demands, KSAs, and standards are not asked separately for individual tasks, but participants are encouraged to comment on their responses if they wish. In sum, while the structured format of the questionnaire adds consistency to the gathered data

for comparison, the interview mode of administration provides flexibility and creates opportunities to gain context for the work roles.

3 Expected Outcomes and Conclusions

As noted earlier, the two-fold goal of this work is to first develop a cyber aptitude test and to then investigate its application to selecting for different work roles – tool developers, interactive operators, and exploitation analysts. The questionnaire was designed to support the completion of both goals. In order to ensure that the aptitude test battery measures all of the cognitive capacities that are relevant, we need to know how prominent each of the various cognitive constructs is across all of the work roles of interest. This will be done by analyzing the gathered data in aggregate. At the same time, because data is being collected from representatives of the different work roles, analyzing it comparatively between them should highlight the differences in cognitive demands associated with each role.

In conclusion, although there has been copious work done, by a number of experts to map the space of cyber operations, our analysis of documented work role descriptions repeatedly led back to issues of granularity – that too few details about steps involved in operations make cognitive analysis unreliable. No doubt this is partially due to the large volume of operations and expertise that must be coordinated to achieve cyber security. Future steps for this work will be to evaluate the effectiveness of the questionnaire instrument for distinguishing the work roles at the appropriate level, and perhaps to apply it to a wider sample of work roles.

References

1. The National Cybersecurity Workforce Framework, National Initiative for Cybersecurity Education (NICE), http://csrc.nist.gov/nice/framework/
2. Homeland Security Advisory Council Cyberskills Task Force Report: Fall 2012, https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf
3. Yen, J., Zhong, C., Liu, P.: Cognitive Process. In: A. Kott et al. (eds.), Cyber Defense and Situational Awareness, pp. 119-144. Springer International Publishing, Switzerland (2014)
4. Zhong, C., Yen, J., Liu, P., Erbacher, R., Etoty, R., Garneau, C.: An Integrated Computer-Aided Cognitive Task Analysis Method for Tracing Cyber-Attack Analysis Processes. In: HotSoS '15, ACM, Urbana, IL (2015)
5. Campbell, S.G., O'Rourke, P., Bunting, M.F.: Identifying Dimensions of Cyber Aptitude: The Design of the Cyber Aptitude and Talent Assessment. In: Proceedings of the Human Factors and Ergonomics Society 59th Annual Meeting, pp. 721-725. SAGE Publications, California (2015)

Cyber Trust IQ

Assessing Aptitude. Creating Pathways. Precise Placement.

Assessing Aptitude and Talent for Cyber Operations

CONTACT

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