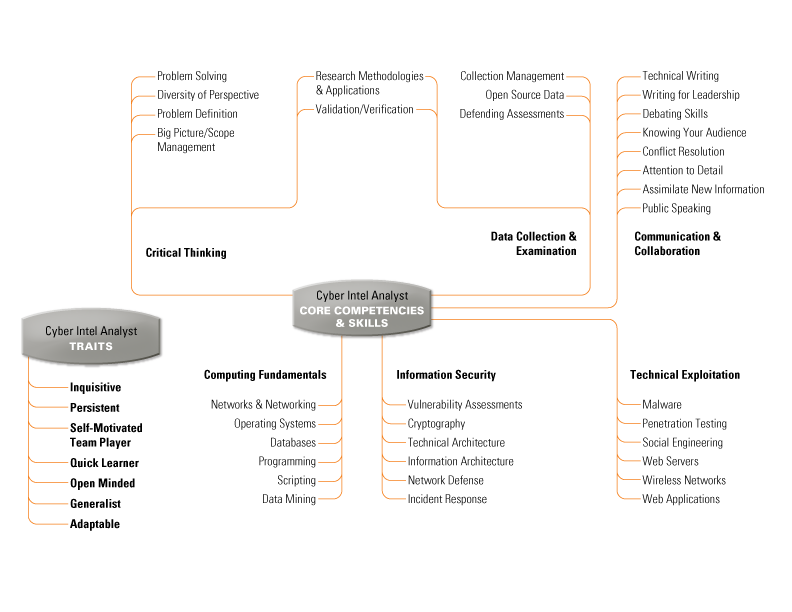
Dennis Devey

May 11, 2017

**Applying Competency Based Education to Introductory Cyber Training**

There is a cyber security skills shortage in the private sector, the government, and the Department of Defense. Everyone wants and needs men and women who can do something about what is happening in cyberspace --there are millions of unfilled security jobs, a constant stream of victims in the news, and dire warnings about the threat to our nation’s critical infrastructure. The cause of this skills shortage is harder to determine than its existence as there are a plethora of offerings that attempt to educate novices. Due to the dominant presence of the information security community online, there are likely more educational resources about the topic floating around than any other specific subject. Yet, decades later there is still no standardized way novices should be trained in order to be successful in the cyber domain. Competency based education delivers a unique approach to this problem because of its focus on measuring ability and promoting self-paced advancement. By identifying the critical competencies required to help students achieve the required baseline level of knowledge and ability and applying learning principles to teach those competencies, educators can build an optimal framework to prepare new students for success in the cyber domain.

Currently, there is no lack of resources or routes for someone hoping to enter the field, but because there is no clear starting point or path to follow many are forced to find their own way. Countless new students attempt to self-teach the wealth of publicly available material that can be found online, oftentimes because many introductory guides recommend that route. New students are overwhelmed when faced with a litany of ideas and concepts they have never seen before, and feelings of being out of place rapidly manifest which results in a high attrition rate. Students are often discouraged at the slow pace of progress and the sheer amount of knowledge it appears they have to learn before they can participate in any meaningful way. In addition, the student misses out on the strength and knowledge of the community and the help they can gain from people who have faced the same challenges before. Those who teach themselves also find that it is difficult to demonstrate that they possess the required skill sets to a prospective employer. Digital classes from massively open online courses provide a more structured curriculum, offering microdegrees and certificates of completion. They are a step in the right direction, but rarely offer the sense of community and support required, or a comprehensive long term plan. In addition, very few of those certificates carry any weight in the hiring process. In order to address the difficulty of demonstrating knowledge, a series of organizations have developed the required reputation to bestow authoritative certificates on anyone who takes their expensive tests. Certificates solve the problem of demonstrating knowledge to an employer, but often fail to help students learn knowledge at the depth of understanding required to be successful. The only educational route that offers a long term plan is an undergraduate education, but that plan rarely attempts to develop operational ability and is highly inefficient. The amount of knowledge gained in class does not justify the length of time required to complete a four year undergraduate degree, not to mention the prohibitive cost. In many cases, taking individual courses at a community or for-profit college will allow for a cherry picked education that can match an undergraduate degree. With that said, almost all government security jobs and many private sector jobs require some sort of undergraduate education so college can wind up being necessary for advancement in those sectors, despite its inefficiencies and general failure to impart the required skills.

An essential component of designing a curriculum is identifying what the desired end state is. In the framework described in this proposal, the goal is to provide the baseline knowledge needed for an individual to be successful in the field, no matter what their job title winds up being. Over the years, many have tried to summarize the knowledge or skills required to become competent in this field. Of these, one of the most well researched and comprehensive lists comes from Carnegie Mellon’s Cyber Intelligence Tradecraft Project (CITP).[[1]](#footnote-1) While the project was intended to identify the core competencies and skills required for cyber intelligence analysts, the items listed form the core competencies and skills for anyone hoping to participate meaningfully in the cyber domain.

“Cyber Intel Analyst’s Core Competencies and Skills” [[2]](#footnote-2)

CITP takes a unique approach by attempting to identify key personality traits that are a precursor to success in this field. Due to the sheer amount of knowledge required for situational awareness, prospective students who are self-motivated and driven to learn as much as possible are significantly more successful. It is essential for a student to realize that learning everything in the rapidly expanding field is ultimately impossible, but not an excuse to be ignorant of material required for them to be successful. Students must be able to accept that due to the size of the knowledge base, they cannot expect to ever be familiar with all of the things they need to do their job and will necessarily spend much of their time researching and learning as they go. The goal of a cyber education should be not only to teach the technical competencies but also develop the traits required for students to teach themselves whatever they need to learn for the task at hand.

A second characteristic that makes CITP’s framework unique is that it recognizes and assigns the proper emphasis that must be placed on ‘Critical Thinking’, ‘Data Collection and Examination’, and the interplay between those topics.[[3]](#footnote-3) Those skills are ones that will be used on an everyday basis no matter an individual’s role, and while a working knowledge of ‘Computing Fundamentals’, ‘Information Security’, and ‘Technical Exploitation’ is critical, their primary utility is derived from their ability to be applied to data from real world scenarios. And while understanding data and making the correct technical decisions is important, without expertise in ‘Communication and Collaboration’ it is unlikely anyone will be an asset on whatever team they join. Few jobs allow for a singular focus on developing and applying technical expertise, and people who fill those positions are isolated into a very small subset of roles. For everyone else, success demonstrating and developing “soft skills” on top of specific technical knowledge is what enables career advancement.

In order to create a curriculum to achieve the competencies listed, an educator must first understand what a competency is. Competency is defined by the Merriam-Webster Dictionary as “having the necessary ability or skills: able to do something well or well enough to meet a standard”.[[4]](#footnote-4) Competency is not an abstract concept, but rather a measurable standard to be achieved. While there were earlier papers that applied the idea of competency to education, one of the most cited pieces on the subject is the 1974 paper *“Testing for Competence Rather Than for ‘Intelligence”* by David McClelland where he attacked the idea of using intelligence tests as the fundamental method of identifying skilled candidates. His primary arguments against them boiled down to the idea that tests predict test-taking success in school and have little correlation to success in the workplace, that intelligence tests rarely focus on identifying traits critical for job success, and that those tests are inherently biased towards those who are afforded the ability to prepare for them. He aimed to minimize initial inequality, while simultaneously allowing high achievers to set their own pace and develop real world skills.[[5]](#footnote-5) Instead of passing students through the curriculum based off of time served, without ensuring they know the required material, this method ensures that students only proceed upon demonstrated mastery, setting them up for future success and guaranteeing qualified graduates. While his original paper was directed mostly towards college admission tests, the solutions he wound up proposing have been applied across various educational disciplines. He proposed five characteristics for this new method of testing:

1. The best testing is criterion sampling.
2. Tests should be designed to reflect changes in what the individual has learned
3. How to improve on the characteristic tested should be made public and explicit.
4. Tests should assess competencies involved in clusters of life outcomes
5. Tests should involve operant as well as respondent behavior

From his paper, over the past few decades the concept of building a curriculum to help students attain competency in various fields developed and became known as Competency Based Education (CBE).[[6]](#footnote-6) While CBE can take on many forms, it usually is a framework where learners are taught one competency at a time, advancing to the next upon successful completion of each, with a focus on development of concrete skills rather than abstract learning. These branches of competencies are often arranged under one central core competency, building a tree-shaped framework for students to work through at their own pace.

While there is no single defined criteria for what CBE has to be, at a summit held by the International Association for K-12 Online Learning in 2011, a working definition for competency education was created:[[7]](#footnote-7)

1. Students advance upon demonstrated mastery
2. Explicit and Measurable Learning Objectives Empower Students
3. Assessment Is Meaningful and a Positive Learning Experience for Students
4. Students Receive Rapid, Differentiated Support Based On Individual Learning Needs
5. Learning Outcomes Emphasize Include Application and Creation of Knowledge

These design principles can be examined more in depth but various important ideas can be taken away from each.[[8]](#footnote-8) [[9]](#footnote-9) From the first, competencies must build upon each other and move in a logical flow, allowing students to learn, demonstrate, and move on. Secondly, the criteria for success must be laid out in advance, allowing students to identify what they need to do in order to demonstrate understanding or mastery. By clearly laying out the defined end states, students know what needs to be accomplished and are empowered by the ability to self-improve. Three, the defined end states must be measured by meaningful and positive assessment, with the goal of the students working through, but enjoying the test. After completion of each assessment, the student must receive feedback on how they did, as well provide feedback on how they worked through the assessment. This allows for fine tuning of the training and for identification of weak points in student knowledge and skills at the time of assessment. The fourth design principle means that there must be ways to track student progress, identify where problems exist, and provide multiple modes of addressing those problems so that the student can move on. Finally, adhering to the fifth principle means that the assessments must be about applying or developing knowledge rather than recall. The value should be derived from forcing new thought processes and teaching a lesson. Curriculum development is meant to be an iterative process that is refined over time, allowing educators to optimize training modules as well as update the assessments themselves in order to ensure the necessary skills are being taught. The ultimate goal of CBE is to streamline the system so that the resources to succeed are always available to the student but each challenge provides an effective assessment of their ability to apply their skills.

While these principles are important by themselves, various other considerations must be made before applying it to cyber education. First, the curriculum must recognize that students will enter the training pipeline at very different skill levels and that the speed each student moves through must not be dependent on other people. The curriculum must not assume any knowledge or it will risk losing otherwise capable students who will feel out of place and left behind. In addition, students may also have limited time to learn, which could mean they are available only a short period of time each day or at random hours. To address leaving these students out, the curriculum must ensure that they have remote access to material at all times, as well as instant remote access to teachers whenever possible. Secondly, it is important to identify that the single best predictor of success in the information security field is the ability for the learner to recognize a lack of knowledge and take proactive action to address that shortcoming. As a result, in order to optimize resources allocated to each student, it is recommended that there be a non-technical screening process for desire and willingness to learn before teachers offer real time support to students. If a new student is unwilling to spend the time required to learn and research their problems independently before asking for help, it is highly unlikely they will ever be successful in the field. Finally, it is essential for educators to clearly define expectations for students and teach them that there is no problem with never having seen a word or heard of a concept before. By doing this, educators can develop a positive culture of progressive learning rather than a spraying a firehose of technical jargon at increasingly dejected students.

The cyber domain is so interconnected and expansive that there is little chance of an expert knowing everything that they need to do their job on a day to day basis, much less a novice. A technical baseline is required to be successful, but for people who operate in this domain the majority of time is spent doing research and applying critical thinking to the complex interactions that occur at the boundaries between areas of knowledge. As a result, education that intends to prepare a student for success in this field must emphasize how a student should learn and the right way to approach problems, rather than what to learn and how to solve problems. Competency Based Education is designed to test mastery and develop the desired mindset through assessments, while still being accessible for the new student, which makes it the optimal framework to engineer a cyber education curriculum around.

1. “CITP Training and Education”, *Software Engineering Institute*, Carnegie Mellon University, [Web](http://www.sei.cmu.edu/about/organization/etc/citp-training-and-education.cfm). [↑](#footnote-ref-1)
2. Ibid. [↑](#footnote-ref-2)
3. Ibid. [↑](#footnote-ref-3)
4. "Competency." Merriam-Webster.com. Merriam-Webster, 2017.

   Web. 04 May 2017. [↑](#footnote-ref-4)
5. “Testing for Competence Rather Than for ‘Intelligence’” McClelland, David C. American Psychologist, Vol 28(1), Jan 1973, 1-14. [↑](#footnote-ref-5)
6. “Competency-Based Learning or Personalized Learning”, U.S. Department of Education. [Web](http://www.ed.gov/oii-news/competency-based-learning-or-personalized-learning). [↑](#footnote-ref-6)
7. “What Is Competency Education?” International Association for K-12 Online Learning. [Web](http://www.inacol.org/news/what-is-competency-education/). [↑](#footnote-ref-7)
8. Ibid. [↑](#footnote-ref-8)
9. “Detailed Definition of Competency Education” *Competency Works*, PB Works. [Web](http://competencyworks.pbworks.com/w/page/67945372/Detailed%20Definition%20of%20Competency%20Education). [↑](#footnote-ref-9)