In his book *America the Vulnerable*, Joel Brenner states that the People's Liberation Army (PLA) of China has developed a cadre of 30,000 cyberspies, who are supplemented by more than 150,000 “private sector” cyberexperts “whose mission is to steal American military and technological secrets and cause mischief in government and financial services” [5].

Kevin Mandia of Mandiant, an information security firm, says his firm needs a six to eight year investment to develop a cyber-security professional for his company's needs. There are numerous examples in addition to literature support for the notion that cybersecurity education needs to refocus on depth as opposed to breadth. The field of cybersecurity professionals today is evolving from self-taught practitioners to individuals with measured in-depth skills and specialties as varied as sports and medicine. Also, the potential impact of a cybersecurity failure requires cybersecurity professionals to attain a high degree of performance quickly as organizations cannot endure failures as they wait for their employees to improve their tradecraft.

Over the past decade, more than 140 schools have become Centers of Academic Excellence in Information Assurance Education (CAE/IAE). All CAE/IAE schools must map their curriculum to government information assurance standards. While these standards provide a broad approach to teaching cybersecurity, employers increasingly desire depth and breadth of knowledge. New standards, such as the National Institute of Standards and Technology (NIST) National Cybersecurity Workforce Framework [16], provide an increasingly detailed set of knowledge, skill, and ability (KSA) level requirements that is measurable.

However, adding some elements of depth to the current model of teaching cybersecurity is inadequate. We need to begin developing and measuring cybersecurity skills well before college to develop cybersecurity experts. Also, developing and measuring cybersecurity skills cannot be accomplished through traditional academic methods alone, there must be support for students to work independently and in teams along with a competition landscape to test and reinforce skills.

In other fields, performance measurement through real-world scenarios is a key indicator of skill mastery. In this paper, we will show how the NIST National Cybersecurity Workforce Framework and models developed for sports can provide hands-on real-world skill development and measurement for cybersecurity education.

**HOW DEPTH IS ACHIEVED TODAY**

According to Gladwell, the common denominator to get to 10,000 hours of experience is “some sort of special opportunity for practice [10].” Gladwell’s examples are diverse and include the Beatles and Bill Gates. In the case of the Beatles, they performed live an estimated twelve hundred times before they achieved success in 1964. In the case of Bill Gates, during one seven-month period in 1971, it is estimated that the 16 year-old Gates and his cohorts used 1,575 hours of computer time [10]. In both cases, luck, timing, and tremendous individual initiative drove the Beatles and Bill Gates to achieve 10,000 hours of skill development by the time they reached 21 years of age.
The Case for Depth in Cybersecurity Education

While those with a passion for programming today can hone their skills on a personal computer, an environment to support learning and testing vulnerabilities in an operating system or application is not easily accessible. It requires a willingness to break software running in a production environment, not build software in a development environment. If one is not working as a cybersecurity practitioner, there are few “safe” places to learn prior to attending college. However, as with Gladwell’s examples, there are individuals that use luck, timing, and initiative, to achieve cybersecurity depth without college.

Kyle Osborn is an example of an individual who achieved depth in cybersecurity skills without college. Osborn is currently a penetration tester at AppSec Consulting, where he specializes in web application security, network penetration, and physical assessments. Before he turned 21, Osborn was featured in the Los Angeles Times and Business Week as a young cyber warrior. Osborn has attended DefCon, the hacker conference mecca held in Las Vegas, since he was 16. Now 22, Osborn has logged close to 10,000 hours of hands-on cybersecurity experience, much of it as a penetration tester and vulnerability researcher. Osborn’s LinkedIn profile lists college work at Golden West College, Coastline Community College, and Cypress College. However, few if any of his 10,000 hours related to college coursework.

Another person achieving 10,000 hours of cybersecurity depth at an early age is Joe Luna. When Joe was 14, he received his first computer and found it completely fascinating that it could talk to any computer in the world. Joe was home schooled and for the next 3 years spent up to 12 hours a day, or over 6,000 hours, exploring other computers and networks. Joe was an industry professional before turning 18, and today is managing partner of a security company.

| TABLE 1: ACHIEVING 10,000 HOURS IN CYBERSECURITY BEFORE COMPLETING COLLEGE |
|---------------------------------|------------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
|                                | 7th Grade | 8th Grade | 9th Grade | 10th Grade | 11th Grade | 12th Grade | Freshman | Sophomore | Junior | Senior |
| Starting in College             | 0         | 0         | 0         | 0         | 0         | 0         | 2500      | 2500        | 2500    | 2500   |
| Starting in High School         | 0         | 0         | 1000      | 1000      | 1000      | 1000      | 1500      | 1500        | 1500    | 1500   |
| Starting in Middle School       | 500       | 500       | 1000      | 1000      | 1000      | 1000      | 1250      | 1250        | 1250    | 1250   |

EXPANDING DEPTH TO MEET CURRENT NEEDS

Some individuals have taken the initiative to develop their cybersecurity skills on their own, but there is a need for tens of thousands more with the “right stuff.” Both national security concerns and corporate losses related to cybersecurity require a pipeline of specialists but how can a person graduate from college with 10,000 hours of practice? Table 1 shows different ways to achieve this goal.

As the table above shows, simply by sheer number of hours, those starting to develop cyber-security depth during college have a much greater challenge. Two thousand five hundred hours of practice for each year of college would require about seven hours a day. Starting in high school with 1000 hours each year would require about three hours of practice a day in high school and about 4.5 hours per day in college. Starting with 500 hours a year in middle school, or 1.5 hours per day, could mean about three hours a day in high school and about four hours per day in college.

STEM, computer science, and cybersecurity curricula can provide a way for students to learn basics of cybersecurity. However, just as physical education in schools focuses on general health, formal curriculum focuses on breadth of knowledge. A way to develop cyber athletes is needed.

It is not uncommon for middle school athletes to practice and play their sport 10 hours a week, or high school athletes to average 20 hours a week of practice and performance. A 13 year-old seeking to develop depth in cybersecurity would require a similar commitment. Formal school curriculum in cybersecurity is virtually non-existent and appropriate practice fields are in their infancy.

Fortunately, early structured paths to develop cybersecurity depth prior to college are becoming available. One such program is CyberPatriot, a National Cyber Defense Competition. CyberPatriot enables high school students to develop hands-on cybersecurity skills through a team competition sport [7]. CyberPatriot requires students to harden Windows and Linux operating systems images in a time-based competition. At an individual level,
CyberFoundations is an entry-level competition focusing on the fundamentals of cybersecurity: networking, operating systems, and systems administration [6].

CyberPatriot started in 2009 with seven JROTC teams and one Civil Air Patrol team. As of fall 2012, there were over 1200 high school teams playing CyberPatriot. CyberFoundations started in 2010 with three public high schools as the California High School Cyber Challenge. Today, CyberFoundations runs in spring and fall, used by students at high schools across the country.

At the college level, the National Collegiate Cyber Defense Competition, National Cyber League, DC3 Forensics Challenge and other local, regional, and national competitions are available for college age students. Such challenges are critically important to help students develop knowledge and skills that will allow them to be successful in college. Such programs are also critically important to allow colleges to recruit students who are already aware of the field they are pursuing and possess a baseline of skills. In academics, sports and many other areas, colleges and universities require pre-college preparation. This preparation helps to ensure that students have a baseline understanding of their field of study, which increases retention and success in the program. This also serves to raise the skill level of incoming students, allowing academic programs to increase expectations and enhance programs accordingly.

ANALOGY
Evaluating a cybersecurity professional is similar to training a pilot, an athlete or a doctor. Time spent on the task for which the person is being prepared is critical for success. The common theme between all of the analogies for cybersecurity education is that they represent a set of complex tasks that require a high degree of mastery to gain success.

Competitive sports offer a great analogy for cybersecurity education for several reasons. First, sports require a high degree of mastery to gain success and the value of teamwork is easy to see and verify. Second, most students in the United States are familiar with sports and many of these students have already participated in sports giving them firsthand experience that will make the analogy more relevant. Third, sports play out in a competitive landscape. It is impossible to attain complete mastery and perfect accomplishment because there is a competitor that will change his or her actions to reduce the effectiveness of their opponent’s actions.

The sports analogy provides many important insights for cybersecurity education. Perhaps the most important insight is the need for skills development before college. Students do not show up to college untrained and unskilled seeking to become college athletes. Students start their athletic training much earlier in life and by the time they enter college as an athlete they have already spent thousands of hours in training and competition environments, students can begin to determine if cybersecurity is an area they wish to pursue. Schools that wish to foster this activity and seek a competitive advantage for their students can offer related courses and student clubs to augment and support skills development. With one and a half hours of practice per day in junior high school and three hours of practice per day in high school a student can amass more than 5,000 hours of experience before entering college.

Online high school cybersecurity competitions are already available through the CyberPatriot program giving students the ability to gain knowledge, develop skills and compete with others to build, test and then augment their skills. The growing success of the CyberPatriot program is testament to the desire among students for cybersecurity training. CyberPatriot also demonstrates that students are ready to learn and compete in the cybersecurity field and that pre-college cybersecurity preparation is possible.

Athletic training is of great value even to athletes who are not selected or choose not to move forward to the next level. Through strength, training and conditioning students gain enhanced physical fitness, strength, balance, teamwork training and other benefits that will help them in future endeavors. A student who does not move forward to the next level of competition still has developed a work ethic and can better compete in future opportunities. The same is true in cybersecurity education as students develop work ethics, work with team members and gain skills in operating systems, databases, programming and many other areas that will serve them well throughout life and prepare them for other careers requiring information technology savvy. This can further help with the shortage of technically skilled workers in the US labor market.

INTEGRATING EXTRACURRICULAR AND CURRICULAR DEPTH IN CYBERSECURITY
Turning cybersecurity into a team competition sport has advantages of learning through real-world simulations with the ability to track performance. If we can combine the social support and passion a sport provides with grounding and concepts of a cybersecurity curriculum, we can attract more students and make the goal of 10,000 hours achievable for many more of them. This process will provide richer knowledge acquisition, enhanced skills development and confidence that can only come from personal achievement. Participation in traditional high school sports has grown...
In addition, competitions provide a mechanism for maturing the field. The phrase “necessity is the mother of invention,” whether attributed to Aesop or Plato, is close to 2500 years old and cybersecurity competitions create the need to invent new and novel methods in the field. Anyone who has participated in a cybersecurity team knows firsthand the level of effort that goes into understanding how to exploit or protect systems. There is no way to know what the opponent will do which means there is no way to assure success. Each team must put everything it has into preparing new and better techniques and hope their efforts are adequate to bring about success. This process is so active that cybersecurity competitions can never be truly repeated. Teams learn and improve so much at each event that cyber competitions must continually increase the level of complexity. By monitoring the teams involved in competition, competition organizers gain the insight needed to enhance the difficulty of the next event. So it is the competitions themselves that both measure skills and map a path for advancing the field.

THE NIST CYBERSECURITY WORKFORCE FRAMEWORK

The goal of the National Institute of Standards and Technology (NIST) Cybersecurity Framework [16] is to define knowledge, skills and abilities (KSAs) to develop and measure a cybersecurity workforce. The NIST National Cybersecurity Workforce Framework consists of seven categories. Under each category are specialty areas. Under each specialty area are relevant KSAs. Mastering KSAs requires hundreds and perhaps thousands of hours of relevant practice and performance measurement.

Two KSAs for one area (Protect and Defend), one specialty area (Computer Network Defense (CND), Infrastructure Support) appear in Table 2.

These KSAs are mapped today in multiple specialty areas to skills used in cybersecurity competitions, with NIST NICE working to expand their use and correlation in these activities [14]. Diagram 2 shows the learning requirements to gain proficiency in “Protect and Defend” which is one of the seven categories of the NIST NICE framework. A beginner starting in quadrant 1 must learn about the four specialty areas that are a part of the Protect and Defend category. At the same time, the beginner

### Table 2: NIST NICE Cybersecurity Framework KSA Examples

<table>
<thead>
<tr>
<th>KSA Statement</th>
<th>KSA Competency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g. application of defense-in-depth)</td>
<td>Information Systems/Network Security</td>
</tr>
</tbody>
</table>
must start to gain proficiency in the 54 tasks and 143 KSAs that are part of the Protect and Defend category. Learning about the four specialty areas (breadth component) can be achieved through reading and memorization. The tasks and KSAs, however, require a great deal of time to complete as the learner must actual carry out the tasks and related activities. Gaining mastery of the tasks and KSAs can be achieved through performance-based activities, such as competitions.

The NIST NICE framework provides the basis to link effectively knowledge-based (breadth) learning with the appropriate skills-based (depth) learning making it possible to map a set of learning objectives and experiences that lead to a high level of expertise.

** глубина**

**Научное сочинение**

Академическая литература предлагает ценный взгляд на роль глубины и величины в образовании. Библиотека И. Л. изучала эффект глубины и величины в девятом классе на примере искусства и предложила это определение для глубины, “[a] teaching program which allows a sustained long-term concentration in one specific area of study. There may be variety within this area but the different activities are such that they permit an easy transition from one problem to another [4].” Этот общий подход согласуется с нашими обнаруженными в литературе определениями и может быть самым простым для поддержки широкого диапазона подходов. Величина определяется Бишель и А. как “[a] teaching program in which a variety of well-chosen subjects and activities are dispersed in such a way as to accommodate differences in the interests and experiences of the pupils [4].”

**Diagram 2: Cybersecurity Depth vs. Breadth**

Depth can be supported and even inspired in a classroom; however, students must take what they learn and apply it independently. Classroom experiences that support depth must focus on the learner as opposed to the instructor; they must offer continuous assessment with rapid feedback and the ability for the learner to focus and direct their own learning to meet current tasks. Learning requirements for depth must be flexible and always expanding keeping pace with industry, learning to deal with last year’s cybersecurity challenges is insufficient. Through competition and other mechanisms, students must face current challenges and learn to devise solutions in the face of a changing landscape. In the following sections, we define depth as it applies to cybersecurity education and focus on its value and the need to develop a repeatable and sustainable process that leads to depth in cybersecurity skills.

**DEEP AND BREADTH IN CURRICULAR AND EXTRACURRICULAR DEVELOPMENT**

Developing capabilities that meet the ever growing and changing demands of the cybersecurity discipline requires a new approach to the process of educating students. Cybersecurity education today begins at college for most students and focuses on breadth. Breadth is appealing as it is primarily concerned with knowledge acquisition, it is easily taught in an instructor-centered model and it can be fit neatly into courses making it ideally suited for a traditional classroom. Depth, on the other hand, focuses on the ability to apply effectively one’s knowledge and skills to an authentic real-world problem. Depth cannot fit into a traditional classroom and does not fit into an instructor-led approach.

**LESSONS FROM THE LITERATURE**

Academic literature offers some valuable insight into the role of depth and breadth in education. Beittel et al. investigated the effect of depth vs. breadth in a ninth grade art class and offered this definition for depth, “[a] teaching program which allows a sustained long-term concentration in one specific area of study. There may be variety within this area but the different activities are such that they permit an easy transition from one problem to another [4].” This general definition is consistent with most definitions we uncovered in the literature and is perhaps the easiest to apply to a wide range of disciplines. Breadth is defined by Beittel et al. as “[a] teaching program in which a variety of well-chosen subjects and activities are dispersed in such a way as to accommodate differences in the interests and experiences of the pupils [4].”

A 2009 Washington Post article covering the debate between depth vs. breadth in science education defined depth as focusing on a few topics so students have time to absorb and comprehend the subject vs. breadth as covering every topic so students get a sense of the whole and can later pursue those parts they find interesting [12].

Perhaps the most conclusive evidence from the literature on the value of depth in education comes from a study of college science students. Schwartz et al. studied more than 8,000 students at 45 universities and found compelling evidence demonstrating that students whose high school science courses focused on depth as opposed to breadth outperformed the students whose preparation was breadth-oriented [15]. Or, put another way, covering fewer topics in depth in high school science better prepared students for college science compared with covering a broader number of topics. Likewise, a study of the earning power of high school graduates...
The Case for Depth in Cybersecurity Education

in London demonstrated that depth yields more jobs and greater earning potential than breadth [11].

We conducted a limited literature review using the key words “depth, breadth and education” to search against all words in articles in EBSCO and ProQuest. Article titles were examined to determine if the article was referring to depth and breadth in an education context. The first one hundred articles found to match these criteria were examined and 82 of the articles argued for greater depth in education while none called for expanding breadth. Searching specifically for articles supporting breadth would result in many hits. Therefore, the outcome of our literature review does not provide a complete picture although we believe the outcome is interesting nonetheless. The selected articles ranged in dates from 1961 to 2012 and two underlying messages were consistent throughout, namely the fact that teachers and some students prefer breadth but external measures indicate that depth has greater value.

DEPTH AND ITS IMPLICATIONS FOR SELF-EFFICACY

Bandura argues that self-efficacy, a person’s belief in his or her ability to execute a task at a required level of performance, is an important factor affecting one’s ability to attain a goal [3]. Performance accomplishment is the most important determinant of self-efficacy which refers to having performed the same, or similar, task in the past [2]. Learning from a book, memorization of facts and other educational pursuits offer limited support in building self-efficacy.

The outcomes of self-efficacy are critically important since individuals are more willing to take on a task they judge themselves capable of successfully completing [1]. High self-efficacy also encourages increased attention and effort on a task, increased persistence when facing obstacles or adverse experiences and heightened performance accomplishment [1].

In short, to gain self-efficacy in an academic or training environment an individual must perform the task at hand in a way that is most similar to the real-world environment for which they are preparing. High self-efficacy in turn leads to improved performance outcomes. The positive outcomes of self-efficacy have proven to be important in training and education programs that focus on depth in areas including pilot training [8], sales training [9] and many more.

CONCLUSION

The value and need for focusing on depth in cybersecurity education is clear. With incoming students who possess more than 5,000 hours of experience in cybersecurity, colleges can completely redevelop cybersecurity programs to build upon these skills. With such skills, students will be able to work in meaningful internship and cooperative programs in industry attaining firsthand experience with the “real world.” The final result will allow students to develop mastery and industry preparedness helping them to hit the ground running and to provide significant contributions right out of college. The six to eight year employee training noted by Mandiant will be greatly reduced to training just for the unique attributes of specific companies and industries. There is also a benefit that it may attract more students into STEM fields and technical degrees… what the U.S. needs.