Report on Cyber Security Education Project
June 9, 2014

For Further Information:
Dennis Egan: deegan@dimacs.rutgers.edu
Fred Roberts: froberts@dimacs.rutgers.edu

Table of Contents

`

Executive Summary

This report documents the findings of a research project conducted by CCICADA on behalf of the Cyber Security Division (CSD) of the DHS Science & Technology Directorate. The project has a broad charter to research what is currently being done in cyber security education and training, and make recommendations for further research that may be needed to help DHS meet its high priority responsibilities concerning cyber security in the United States.

The project team gathered a wealth of information about ongoing efforts in cyber security education and training. The team convened a brainstorming workshop that brought together fifty-three people including experts on various aspects of cyber security, education, and related disciplines for presentations and discussion in six panel sessions. Input from the workshop and an extensive literature review was organized in a matrix that has as rows the different target student groups that emerged from the brain storming session and further discussion, and as columns different aspects of the educational/training effort. Extensible, interactive taxonomies of major topics in cyber security were prototyped. Additional experts were contacted for input and feedback by phone interviews and email surveys.

The analysis of this vast amount of information led the team, working with other experts, to consider four clusters of questions and to develop key insights within each cluster:

- **What are the implications of the evolving nature of cyber security threats and responses?** The body of cyber security knowledge cannot be static but must allow for dynamic adaptation and extension. This will allow users of iPads and smartphones, as well as users of social media such as FaceBook and Twitter, to have personalized learning/training related to their devices and the way they use them. As new research allows Recommender Systems to become more and more sophisticated, we can expect such personalized learning/training to be expanded to all kinds of contexts, whether for unsophisticated or sophisticated users. A key insight relevant to the evolving nature of cyber security threats and responses is the fact that a number of other disciplines, notably medical education, public health education, engineering, and business education are facing similar issues. There is much to be learned, for example, from universities addressing how to rapidly transition medical research into the curriculum, how to keep practitioners current, and how to apply technologies including simulation, distance learning, and learning management systems to help keep up with the speed of technological change.
- **What are the approaches to cyber security education and training in different communities and organizations?** Cyber security training must be appropriately tailored to one's job or position in an organization, and for K-12 the tailoring must be appropriate

to a student's level of development. A second insight is that there is no currently agreed upon body of knowledge that would constitute a cyber security curriculum. This is not necessarily a bad thing, as the field is evolving and it is important for different institutions to be experimenting with different approaches. However, it is also important to be working toward some models that can be widely emulated, which would make it easier for students to switch from one program to another or one institution of higher learning to another, which right now is a challenge due to differing programs and requirements. While cyber security may not be mature enough yet as an academic discipline, it is possible and very desirable to work cyber security topics into other degree programs, including not only STEM degree programs, but also a broader range of degree programs including law, economics, business, social science, political science, and criminal justice.

- **What principles of teaching and learning are applicable to cyber security education and training?** Long-term retention and transfer are particularly important learning outcomes for cyber security training and education, because the application of cyber security knowledge is likely to occur long after the initial learning takes place and in future contexts that cannot be fully anticipated. Although further research is required, teaching principles based on constructivist and experiential learning theories appear likely to lead to successful long-term retention and transfer. These principles are consistent with the reported benefits of cyber security students working in teams, and getting "hands-on" experiences in practical projects and internships.
- **How can the effectiveness of cyber security education and training be assessed?** Assessments of effectiveness will depend on the objectives of the specific cyber security education or training program, which can range from simple awareness and literacy up to very detailed technical knowledge and skills. There is a need for research to develop training and assessment tools that can be deployed at the level of an enterprise or agency so that the effectiveness of various occasions for delivering training (e.g. "teachable moments," and repetition schedules) can be tested in the job context.

Recommendations followed from comparing the discussion around these questions to current practice and ongoing projects. Our recommendations first set forth some general principles: fundamentals of education and training in this space; addressing the multiple target student groups; and the timing of various training and education efforts ranging from near-term (within a few months) all the way to ultra-long-term (over many years).

The following summarize our key recommendations. Others are included in the report.

<u>Key recommendations specific to education and training are:</u>

1. Teams: Learn from education and training in other disciplines (e.g. medicine, public health, engineering, business, the military, etc.) how to instruct cyber security students to work in teams and to use their knowledge and experience to address situations never seen before.

2. Internships: Internships are a key way to enhance contextual, on-the-job learning, which is a key component of cyber security education and training and is centrally related to day to day operations in the cyber security role. Encourage the Homeland Security Enterprise (HSE) to develop internship opportunities for college/university students interested in cyber security and faculty teaching cyber security, and work with the private sector to develop cyber security internship opportunities for HSE employees.
3. Module development and certification: Develop cyber security modules for short periods of time that can be used in different courses of study, including in nontraditional disciplines (see next recommendation) and for the generalist, not just the specialist in cyber security.
4. Engage more disciplines: Put increasing emphasis on additional important topics for cyber security education such as learning science, psychology, sociology, economics, political science.

Key recommendations for the existing workforce and workforce development are:

1. Sharing information and best practices: DHS could play a major role here in enhancing already-existing approaches to information sharing. We suggest focusing specifically on DHS NCCIC interactions with the ISAC organizations to promote information sharing with the larger HSE. Sharing information and "best practices" is a good way to keep up with evolving challenges. This is especially relevant to "on the job learning" and "adaptive learning" that addresses how today's subject matter expert in one discipline needs to be a life-long learner to keep up with new disciplines and rapidly changing contexts in which to apply the discipline in which they were trained.
2. Cognitive skills goals: Develop specific examples of cognitive skill goals for cyber security experts in terms of knowledge/remembering, comprehension/understanding, application/applying, analysis/analyzing, evaluation/evaluating, and synthesis/creating.
3. Small organizations: Consider the special needs in terms of cyber security education/training for small businesses or smaller agencies in the HSE.

Specific key recommendations for further research are:

1. Defining the Cyber Security Body of Knowledge: Encourage research to establish a definitive body of knowledge for the discipline of cyber security that can aid in curriculum development and potential future accreditation, certification and professionalization efforts.
2. Better metrics for effectiveness: Encourage research to identify metrics for effectiveness of cyber security education and training for each of the student groups described.
3. When and how to begin cyber security education: Encourage research to determine the appropriate age to begin cyber security education and to determine the "sweet spot" at which to start serious exposure to cyber security.

4. Transfer and repetition: Encourage research on alternative modes of teaching to emphasize concepts of transfer and repetition into cyber security education and training for the DHS workforce as well as school settings, and design experiments to test the effectiveness of different modes of delivery and the frequency and spacing of repetitions.

1. Background on Project

Since 2008, DHS has been given broad, major responsibilities concerning cyber security in the United States. As then-Acting DHS Secretary Rand Beers wrote November 13, 2013 for a Senate Committee on Homeland Security and Governmental Affairs hearing, "Over the past four and a half years, cybersecurity has emerged as a top priority for DHS through our efforts to secure unclassified federal civilian government networks, work with critical infrastructure owners and operators, combat cyber crime, build a national capacity to promote responsible cyber behavior and cultivate the next generation of frontline cybersecurity professionals – all while keeping a steady focus on safeguarding the public's privacy, civil rights, and civil liberties" (see Beers, 2013).

The priority and corresponding investment given to cyber security has resulted in some success, but evidence continues to show an increasing number and severity of cyber attacks. On the positive side, DHS has implemented a network intrusion detection and prevention program called Einstein and is implementing a continuous diagnostics and mitigation (CDM) program, both of which are designed to protect the "dot-gov" domain. Through the US Secret Service (USSS) DHS has managed to prevent billions of dollars of losses by stopping some cyber fraud and cyber thefts, and the USSS has successfully arrested thousands of cyber criminals thereby presumably stopping additional large losses. However, cyber attacks continue to increase. The number of cyber attacks reported by federal agencies to the US Computer Emergency Readiness Team (US-CERT) rose by more than seven-fold to almost 50,000 attacks per year from FY 2006 to FY2012 according to a recent GAO report (see GAO13-187). The same report documents recent examples of cyber attacks affecting national security, costing businesses millions of dollars in stolen intellectual property, and threatening the financial well being and privacy of individual citizen, all of which occurred before the theft of over 100 million credit card holders' information from two large retailers in the Fall of 2013.

There are good reasons to believe that improving cyber security education and training of people in the current or future workforce is an important component in deterring cyber attacks now and in the future. An analysis of the FY2012 attacks reported by federal agencies shows that the single largest type of attack accounting for 20% of all attacks was "Improper Usage," an attack that is attributable to users "violating acceptable computer use policies" (GAO 13-187). This finding was reinforced at the Brainstorming Workshop we conducted (see Section 2) where one of our private sector cyber security experts claimed that, "Users are the weakest link in cyber security." Educating and training users in acceptable computer use policies (e.g. creating good passwords and keeping them safe; not clicking on embedded links or attachments in email from unverified sources) can improve the current situation. Additional types of attacks such as

unauthorized access, and scans and probes to access computers via open ports, protocols and services also may be reduced by providing effective cyber security education and training to network administrators and IT staff.

The foregoing examples suggest that cyber security education and training can improve the performance of the current workforce and current cyber security technical staff. Another huge challenge is educating and training a pipeline of students who will become the cyber security workforce in the future. NIST has projected a need for 700,000 new cyber security professionals by the year 2015 for the public and private sectors in the United States alone (see Section 3.3). To meet this challenge requires a concerted effort by the government, the private sector, K-12 educators, and academics at colleges and universities. Much of the material presented in Sections 3, 4, and 5 describe these ongoing efforts, raise questions and issues about them, and make recommendations for further efforts.

The DHS charter for cyber security education and training extends to all students, beyond those in the current and prospective cyber security workforces. It also includes people who are not in any sort of formal training or education program, namely the public at large. It is only by enhancing the education of all students with modules or elective courses focused on cyber security, regardless of the students' area of concentration, that the next generation of citizens can be reached with important information that may help safeguard themselves, their prospective employers, and the nation itself from cyber attacks. Similarly, to reach those either not yet involved with or no longer involved with formal education, DHS must support cyber security and education for the public at large. It is only by educating and training all four groups (the current cyber security workforce, the pipeline of future cyber security professionals, other general education students, and the public at large) that DHS can meet its responsibility to "build a national capacity to promote responsible cyber behavior and cultivate the next generation of frontline cybersecurity professionals" (Beers, 2013).

1.1 DHS' "charge": The Cyber Security Concepts Development Study (CS-CoDeS)

Given (a) the responsibilities of DHS for cyber security, (b) the evidence of continuing serious cyber attacks despite current programs, and (c) the likelihood that cyber security education and training can improve the national cyber security condition, the DHS Science & Technology Directorate Cyber Security Division (CSD) commissioned this Cyber Security Concepts Development Study (CS-CoDeS). The Center of Excellence for Visualization and Data Analytics (CVADA) was asked to draw on a range of team expertise – from areas such as cyber

security, education, operations, analysis, intelligence, and business – to study and develop strategic concepts for how cyber security operations and education could be researched, designed, organized and executed for significant gains in organizational, sector and national cyber security capabilities. This report represents the work of the data science lead for CVADA, the Command, Control, and Interoperability Center for Advanced Data Analysis (CCICADA).

Quoting from the statement of work for the project, "The purpose of the CS-CoDeS is to support CSD's development and consideration of a new research program addressing cyber security education … This research effort will look at trends in a number of existing areas of education, learning and operations research, in cyber security and other technical domains, and develop strategic and architectural concepts for how DHS might approach the coupling of cyber security operations, education and training across key interest areas. This work should consider the different perspectives of government and business organizations; national organizations, such as NCCIC/US-CERT; collaborative environments, such as the frequent intersections of major cities/states/corporations; and large-scale academic environments and organizations. The intention of CSD is to focus initially on developing understanding by DHS organizations, such as US-CERT, NCCIC/NICC, and associated critical infrastructure sectors and Information Sharing & Analysis Centers (ISAC's), and then shift attention toward the challenges of how to take this stronger content and use it to better educate the nation with respect to cyber security."

1.2 Defining the Field of Inquiry

In order to sharpen the focus of this study and to avoid spending resources considering extraneous questions, the team has developed a provisional definition of the key terms *cyber security*, *cyber security education*, and *cyber security training*.

The UMUC cyber security program defines cyber security, or information technology security, as an effort that
"…focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction." (http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfmhttp:/www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm). One expert we talked to insisted that it is important to include the whole lifecycle of security, including questions about design, procurement, configuration, and disposal, suggesting that cyber security is a multi-faceted and multidisciplinary undertaking.

Of course, the ultimate goal of protecting computers, networks, programs and data is to protect the interests of the people or entities invested in these assets.

Thus, cyber security *education and training* can be broadly defined as any effort to equip human beings to carry out this protective role in any context, whether as a full-time career, as part of the duties of an information worker, or simply as the basic responsibilities of a citizen of cyberspace. To us, this includes teaching the knowledge and skills for both *prevention of* and *response to* security breaches.

We believe a significant distinction can be made between the notions of cyber-security *education* and cyber-security *training.* In terms of outcomes, the result of education is an understanding of the concepts and issues involved, while the result of training is a set of skills for using existing tools to cope with some current forms that these issues take. University courses typically are focused on education, and indeed may not have access to current hardware and software tools to carry out training. On the other hand, professional certification courses and courses offered within a specific job context are training oriented, and often specify precisely which tools the trainee will master. In general, education is intended to provide a life-long foundation, while training tends to have a short lifespan and needs to be updated continuously.

However, since virtually every educational program will have both conceptual and procedural aspects, and since both education and training are needed to fulfill the role described by our definition, this report treats both notions, and presents insights we have gained from investigating in which contexts one of the two may receive greater emphasis. This having been said, much of this report applies to both education and training and in most cases we leave it to those using our report to determine how or whether to apply a particular idea or recommendation to education or to training or to both.

1.3 Operational Tasks

Given the scope of research outlined by DHS S&T CSD, CCICADA developed several tasks to operationalize the project.

1.3.1 Task 1: Survey of Cyber Security Education Efforts

We planned to survey cyber security educational efforts in government agencies, including DoD, in selected companies, and educational institutions, including K-12 as well as colleges and universities. We quickly found that we also had to find information concerning less formal educational efforts as well, such as those provided by the Boy Scouts and Girl Scouts, volunteer teachers working with community groups, and public awareness activities sponsored by the National Cyber Security Alliance, among others.

This task also included a search for other disciplines with characteristics similar to cyber security, to find out how education and training is carried out in those disciplines. The salient characteristics of cyber security include the need for specialization, the critical roles of internships and team problem solving, the requirement for education and training beyond the terminal degree, and some kind of professional accreditation process. We have identified relevant education and training models from medicine, emergency medicine, public health, accounting, engineering, and the military and these are discussed in Section 3.2.2 and Section 4.1.2.

The final part of this task was to develop one or more taxonomies of cyber security education topics and resources. Our team devised preliminary versions of three hierarchical taxonomies and prototyped a user-friendly interface for accessing them via an extensible point and click interface. These taxonomies are described in Section 2.3.

1.3.2 Task 2: Brainstorming Workshop

To start a dialogue with experts in cyber security education, with an emphasis on government and the private sector, and to aid in the beginning of data gathering, we planned a "Brainstorming Workshop" at Rutgers in the Fall of 2013. Participants included project participants (students and faculty) as well as experts identified from academic, government, and private sector institutions. This workshop is described more fully in Section 2.1.

1.3.3 Task 3: Engaging Other Universities

The three universities directly involved in the CCICADA Co-DeS project, Rutgers, CMU, and Stevens, are all designated as NSA/DHS Centers of Academic Excellence in both Information Assurance Education (CAE/IAE) and Research (CAE/R). Some 181 schools around the country hold one or both of these designations or designation for two-year institutions (CAE/2Y). As members of that community, the CCICADA faculty involved in the project are already engaged in cyber security education and have extensive contacts with others in that community. Through NSF funding, a number of universities have established programs known as CyberCorps: Scholarship for Service Programs geared to increase the number of cyber security experts in the federal workforce, particularly those with multidisciplinary backgrounds. Such programs, aimed at undergraduate and graduate students in computer science or electrical engineering and other disciplines, provide a comprehensive education in cyber security. Carnegie-Mellon and Stevens have such programs, as does CCICADA partner University of Illinois at Urbana-Champaign. We planned to engage these programs in the initial stages of our planning and in our data gathering. We also made contact with a wide range of universities to

identify programs they are already running. Many key university players were included in our workshop.

1.3.4 Task 4: Exploring Relevance of a Variety of Disciplines

While it is clear that computer science and electrical engineering are particularly relevant disciplines in the cyber security area, there are many others. For example, the CyberCorps programs are multidisciplinary and include areas such as law, economics, business, risk management, and IT. Also relevant are cognitive science, political science, history, sociology, criminal justice, and behavioral science. The need for multidiscipline involvement in cyber security cuts two ways. On the one hand, students pursuing degrees in law, business, economics, etc. need at least a basic understanding of cyber security because its implications are so pervasive for the field they are studying. On the other hand, students who will become cyber security experts need some grounding in law, business, economics, etc. in order to understand cyber security policies and to be able to communicate with others in organizations (e.g. CEOs) who may not have deep knowledge about cyber security. Of course we cannot expect an individual to become expert in so many disciplines. Indeed, there are almost surely disciplines and subdisciplines of the future that will be relevant to cyber security. However, cyber security experts should be trained to work with experts in other disciplines so that they can call upon these disciplines even if not expert in them. Organizations that have the ability to hire teams of cyber security experts can look to have a variety of disciplinary expertise represented. Reflecting our view of the importance of many disciplines, we identified for this project faculty members and experts in other disciplines such as mathematics, information science, education, engineering, economics, and behavioral science to work with us.

2. Methodology

The project team collected information from several sources. A literature review was started with a specific focus on cyber security curricula, methods of delivery, applicable learning and teaching theory, and published reports. We did not try to include the substantial academic research literature on cyber security *per se,* though the team doing the literature review included people knowledgeable about this research literature and who could include selected relevant literature as appropriate. Since cyber security education is an extremely active and rapidly evolving topic, the team decided to invite national experts to a "brainstorming workshop" to understand ongoing work and to help us to focus the project. Results of the workshop led to initial ideas for organizing literature and other references as they were collected. Team members also began to prototype three interactive extensible taxonomies of major topic areas for cyber security education that people could use to access resource materials. The team followed up the workshop by reaching out to specific people (some of whom participated in the workshop) with an email survey and/or phone interview.

2.1 Brainstorming Workshop

For the brainstorming workshop we invited subject matter experts in cyber security education and related disciplines. Workshop participants included a mixture of experts from academia, government, and the private sector. Time did not permit any kind of formal sampling, so we pursued a "snowball sampling" or chain-reference approach in which the team started with experts we knew or knew about and then solicited additional ideas for participants from those experts. Since time was short, we enabled people to participate in the workshop either in-person at Rutgers University, or virtually via teleconference with shared slides. The date set for brainstorming workshop was October 7, 2013 which, as luck would have it, turned out to be in the middle of the federal government shutdown. As a result, participation by federal government experts was somewhat curtailed. The team has supplemented the federal government subject matter experts' participation by reaching out individually to a number of government experts via phone interviews. Fifty-three people participated in the workshop, including experts from around the country and the project team, some of whom are cyber security education experts in their own right (see Appendix 8.1).

The workshop was organized into six panel sessions. Each session consisted of 5-minute presentations by several experts followed by a discussion in which all workshop participants could pose questions to the panel. Each panel was facilitated by a project team member. The titles and themes of the panel sessions were:

1. Government and Industry: What is happening now at government agencies and universities and what might be needed?

2. Private Sector: What is happening now in the private sector and what might be needed?

3. Education Principles of Teaching and Learning for Cyber Security: What general principles of teaching and learning, based on educational theory, will aid us in evaluating and choosing new cyber security educational programs?

4. Learning from Analogies: What can we learn from medical education, public health education for the public, energy-efficient behavior education, education of the military, etc?

5. K-12 and Informal Public Cyber Security Education: What is happening in K-12 and public education including adult education and public informal education?

6. Tools of Delivery for Effective Cyber Security Education: Discuss modes of presentation (online, videos, use of apps), frequency (monthly updates, retraining,), use of technology (games, virtual reality), and tie these in to teaching and learning.

A complete list of panelists and facilitators is presented in Appendix 8.2.

2.2 Matrix Organization of Resources Collected

The literature search, panel presentations, and information collected subsequently via the email surveys and phone interviews presented a challenge simply to organize the huge amount of information coming to the project team. The team developed an organizational scheme that could be used to classify each piece of information, and facilitate a quick scan of the sources collected so that information completely missing or only lightly populated for a given set of topics could be spotted easily.

The team worked through several iterations of a classification scheme before settling on the following matrix:

Population	A: Existing programs targeted at these learners	B: Educational principles that apply to these learners	C: Analogous other kinds of educational efforts	D: Modes of delivering the education	E: Reports on the state of the art for educating this population
1 Public and K-6					
2 Cyber Security Workforce					
3 High School and College Students in Cyber Security Pipeline					
4. Other Students Receiving Cyber-Security-Enhanced Education					

The rows of the matrix are the populations of students requiring cyber security education. The columns are programs (including curricula), educational principles, analogous training efforts, modes of delivering education, and reports on the state of the art.

This matrix has proved useful, but we do not claim that it is optimal. It has proved useful as a shorthand in our email survey to have people classify topics that they are working on, e.g. 2-A or 3-D, etc. It has also served the purpose of letting the team see where we might be lacking information. On the other hand, the project team has repeatedly discussed whether we have the best factoring of the educational populations (the rows of the matrix). Our initial thinking suggested that it made sense to group educating The Public with educating K-6 students. However, given the importance attached by many experts to teaching cyber security in elementary and middle school it probably makes sense to separate the first row of the matrix into three distinct groups (The Public, Elementary School, and Middle School; see Section 4.4.1). Similarly, we later came to see that we might have better had a separate row for the "rest of the workforce," but for purposes of our research we included that in the Cyber Security Workforce row. The matrix with the resources we identified is included in Appendix 8.4.

2.3 Taxonomies of Major Topic Areas

Because of the rapid development of cyber security technology (e.g. both malware and the various kinds of remedies evolve very quickly), it is unlikely that any educational plan's topics will remain complete and up-to-date for long. In order to help educators, current students, and

graduates find the latest available information, we suggest the creation of an external accessible resource that houses relevant information (for example, descriptions, software, discussion groups, blogs, etc.) that people can query to educate themselves when they want to.

The project team has developed small initial prototypes of three interactive extensible taxonomies that can be used to categorize resource materials for teaching and learning about a variety of topics in cyber security education (see http://www.cs.cmu.edu/~dklaper/cybersecurity/website/index.html). The Main Taxonomy (see Figure 1) includes Technical Aspects of Cyber Security such as Data Integrity Verification, Cryptography, Intrusion Detection and Risk Mitigation, Authentication and Authorization, and Auto-Analysis of Legitimate Usage Patterns as well as Impacts of Cybercrime and Cyber Security. The Operational Cyber Security Risk Taxonomy (see Figure 2) includes as its high-level topics Actions of People, Systems and Technology Failure, Failed Internal Processes, and External Events. The User-View Taxonomy's (see Figure 3) highest-level topics includes End-User Focus, Human Resources Focus, Permanent Network Administrator Focus, Legal/Forensics Focus, Financial Impact Focus, and Temporary Collaboration Network Administrator Focus.

Figure 1: The Main Taxonomy

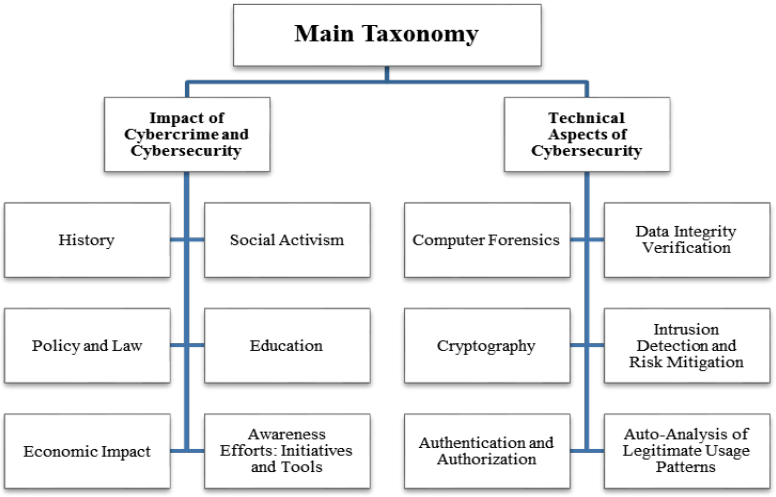


Figure 2: The Operational Cyber Risk Taxonomy

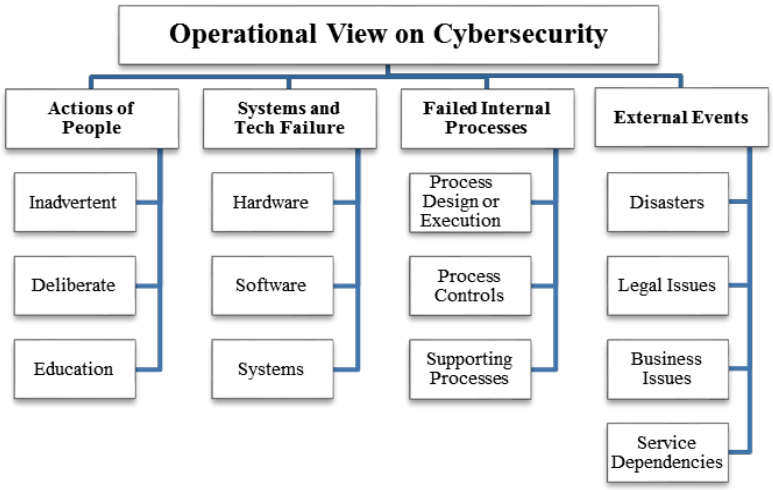
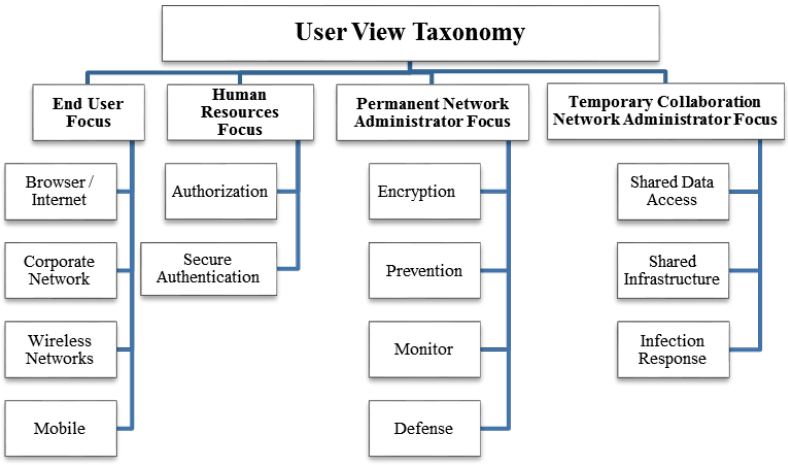


Figure 3: The User View Taxonomy



In each taxonomy, the highest-level topics can be expanded by the user into more-specific sublevels in a topic hierarchy. The taxonomies have a common XML-based structure and metadata format. Users can point and click on taxonomy topics to expand to the next level. At each level the data includes pointers to resource materials (currently, mostly research papers, but ultimately, also laws, procedures, discussions, software, etc.). In addition, each node also gives the path through the hierarchy from the top node to the topic and a definition of the topic.

These taxonomies provide a useful and very usable way to access resource materials for teachers and students interested in particular topics. The taxonomies also could be the basis for a system that could use machine learning to add resources in a semi-automated fashion, and provide a

portal with a query interface (see description of the Personal Cyber Security Assistant / Smart Notes project in Section 4.1.3) so that teachers and students could very quickly find up-to-date resources on cyber security topics of interest.

2.4 Email Survey and Phone Interviews

Following the brainstorming workshop, the project team decided to obtain additional information from subject matter experts via an email survey and/or phone interviews. Our initial emailings attempted to contact people who had participated in the workshop and other experts and proposed that they either reply by email or schedule time for a brief phone interview. Using these methods we were able to fill in some information we were missing, either because some of the experts were not able to provide extensive information in their very short workshop presentations, or were not able to attend the workshop. In other cases, we learned about other experts as part of our project research.

The email survey presented the matrix shown above (Section 2.2) and asked the recipients to respond with a short email providing information on work they were doing relevant to the specific cells of the matrix. The survey also asked specific questions about materials used in cyber security education, and ways to assess effectiveness. The phone interviews have been more free-form, and have been tailored to the specific expertise of the person contacted. We obtained information through 19 email survey responses and phone interviews (sometimes following up an email response with a phone interview; see Appendix 8.3). Summaries of both the email surveys and the phone interviews have been written and provided to all the team members.

3. Lay of the Land

Our literature review, the brainstorming session, and interviews with subject matter experts all indicated a tremendous amount of activity focused on cyber security education. The stimulus for all this activity has been the dramatic increase in cyber attacks especially over the past five years or so. The escalation of these attacks hardly needs documenting here, since they are the subject of news reports on an almost daily basis, and they range from data breaches of personal data to corporate espionage to creation of spam-launching botnets to national security threats (see GAO Report 13-187 for recent data and examples).

There are multiple purposes for cyber attacks. Cyber warfare attacks can be carried out by governments or dissident groups and may focus on damaging cyber physical infrastructure (power networks, SCADA systems, signaling systems, etc.). Cyber espionage attacks may penetrate government computer systems to steal classified and sensitive information related to national security. Cyber crime attacks have targeted private enterprises both large and small to steal customer information, credit cards, and intellectual property, to create havoc by inserting disinformation, and to bring down transactional websites. Cyber crime attacks have also targeted government systems to steal citizens' tax records and other personal information. Personal cyber attacks have been waged on individuals, including children, to steal identities, invade social networks, and to carry out cyber bullying.

3.1 Background

The government, private industry, and non-profit professional and educational groups have responded to the increasing cyber security threats with numerous initiatives aiming to improve cyber security education and training for one or more target populations. We will not try to present an exhaustive list of these initiatives, but will describe categories of such initiatives with some examples of each.

3.1.1 Cyber Security Job Analyses

A number of initiatives are aimed at bringing some structure to the myriad job positions related to cyber security. Such initiatives are important because they could help inform attempts to define curricula for educational programs in cyber security. They could provide the basis for testing proficiencies in various skills and knowledge sets. They could also improve recruiting in cyber security.

One of these initiatives is the NIST National Initiative for Cyber Education (NICE). This is an extensive program one component of which has produced the National Cyber Security Workforce Framework "to provide a common understanding of and lexicon for cyber security work." The Framework consists of seven major job categories further refined into 31 specialty areas supported by a very large number of tasks, knowledges, skills, and abilities (KSAs). While the Framework is the first of its kind and should bring some consistency to job titles in cyber security, more than one of our experts has said that it is unwieldy for the purpose of planning cyber security education and training for the workforce.

Another initiative is the DHS Advisory Council Cyber Skills Taskforce that has recommended an authoritative list of ten *mission-critical* cyber security jobs within DHS. This initiative is extremely important for DHS, because it focuses squarely on those jobs at the center of DHS security operations. A report by Lute, Durrance and Uenumo (2014) reconciles the NICE and Taskforce approaches and relates the mission critical functions to industry job postings and certification courses. Other Taskforce recommendations focus on training and recruiting and educational programs in support of maintaining expertise in those jobs.

A third approach, Job Performance Modeling, has been adopted by the Council on CyberSecurity. This approach follows processes for job definition through several stages ultimately resulting in statistical validation of items assessing the development of expertise. This approach is the most technically sophisticated, but could take a large investment of resources to develop and maintain models for a large number of different cyber security jobs.

3.1.2 Cyber Security Curriculum Analyses

A second set of initiatives has focused on college programs of study that would yield students who would be qualified for cyber security careers. For example, the NSA in collaboration with DHS has established a program of Centers of Academic Excellence in Information Assurance Education and Research. The CAE program has currently designated 181 schools, including 2-year institutions, 4-year institutions, and research institutions providing doctoral studies. These schools have received the CAE/IAE, CAE/R, or CAE/2Y designations. Four-year and designated Information Assurance and Research institutions can apply for grants and scholarships through the Department of Defense Information Assurance Scholarship Program and through the NSF Scholarship for Service Program. Because of the rapidly evolving nature of cyber security, institutions must seek redesignation every two years under updated knowledge unit and core curriculum requirements. Requiring such frequent redesignation is indeed a strength of this program.

A joint committee of the ACM and IEEE has reviewed the overall curriculum for a bachelor's degree in computer science and recommended the makeup of courses required for accreditation

(see ACM/IEEE-CS Joint Task Force on Computing Curriculum, 2013). While this effort is not precisely focused on cyber security, it does have important implications. The new curriculum is broken down into 18 knowledge areas (of which Security and Information Assurance or IAS is one) and the number of lecture hours to be allocated to each area. Currently this reference curriculum specifies that programs must teach 100% of Core Tier 1 knowledge areas which includes 3 hours of IAS, and 80% of Core Tier 2 knowledge areas which includes 6 hours of IAS. Additional hours for IAS are included in the teaching of other knowledge areas (32 Core Tier 1 hours, and 31.5 Core Tier 2 hours), and electives.

The ACM conducted a workshop in 2013 focused specifically on cyber security curriculum and published a report, "Toward Curricular Guidelines for Cybersecurity." The report reviews previous work in this area and examines cyber security curriculum issues for doctoral students, masters students, undergraduates and associate degree students. As noted in the report, there have been other approaches to developing cyber security curricula based on the NICE program, as well as analyses of the most serious and common cyber security defense flaws. The ACM Board currently has a draft report on cyber security education and teaching.

3.1.3 Cyber Competitions

Cyber competitions represent a third, rapidly growing set of initiatives focused on improving cyber security training and education. Cyber competitions offer several attractive features: they do not displace course hours in an academic curriculum; the team competitions can foster learning how to solve cyber security problems in a team setting; and students can develop deep expertise in a specific domain. The National Initiative for Cybersecurity Careers and Studies maintains a cyber competitions repository with descriptive information about competitions. At the time of this report, there are 72 competitions listed. Some are restricted to specific academic levels (e.g. high school or collegiate). Some are restricted to specific geographical areas (e.g. a specific state or region of the US), but others are global in scope. Some are set up for team competition and others are for individuals. A number of the competitions include a job fair in which competing students often are offered cyber security jobs on the spot.

3.1.4 Certification Programs

Certification programs for cyber security represent a fourth set of rapidly growing initiatives. Organizations such as CompTIA, ISC2, and SANS among others all offer cyber security certification programs. The programs are typically offered with various kinds of training, and certifications typically must be renewed periodically. Information security product vendors like CISCO and Microsoft also offer certification specific to their products. There is a debate whether cyber security is mature enough as a profession to warrant an extensive certification program. The National Academy of Sciences studied this issue and suggested that, aside from specific

areas like digital forensics, which is a mature discipline, applying professional certification to cyber security may be premature. According to the report, certification programs also may present barriers to people entering cyber security as a career just at the time that more people are needed. Not everyone we talked to agreed with this conclusion, and in Section 4.1.2 we explore some alternative ideas, in particular certification of more advanced cyber security workers.

3.2 Educating and Training the Current Cyber Security Workforce

In this section we report on efforts to train the existing cyber security workforce in DHS, the US Military, and private sector businesses.

3.2.1 DHS and HSE Workforce

While the need for cyber security employees is critical in DHS, the people we have interviewed told us that DHS lacks the core capabilities to educate and train current employees in cyber security, or hire new employees effectively to fill cyber security positions. As an organization, DHS is barely ten years old and is composed of 22 different agencies. Its training and career structures are not mature. Only a few individual agencies (the Secret Service, Immigration and Customs Enforcement, and the US Coast Guard being examples) have training facilities and established curricula so that cyber security training might be added. This lack of agency-wide training in cyber security is not unique to DHS. The GAO recently analyzed eight federal agencies with the highest IT budgets and found that only three of the eight agencies had a department-wide training program for their cyber security workforce (GAO 13-187).

DHS has made strides recently in providing training on privacy policies to all of its employees, suggesting that its capacity for developing, delivering, and managing training is improving. A mandatory annual online privacy training course is taken by all DHS employees. Student records are maintained for compliance, and the course is updated to reflect changes in privacy policies and feedback obtained from the employees. While DHS currently maintains eight different learning management systems, the plan is to consolidate these to a single system this year. In addition to a department-wide course for all new employees, and the annual refresher course for all employees, advanced courses are offered to employees who handle Personally Identifiable Information (PII) routinely in their work. A variety of course formats (instructor-led, train-the-trainer, online) can be used to deliver courses tailored to specific offices and agencies. The DHS Privacy Office also emails privacy alerts and maintains a website archiving these alerts. This work on privacy training could well form a model for DHS cyber security training. Indeed, to the extent that cyber security training requirements bear some analogy to privacy training requirements, better cyber security training for DHS employees may soon be possible.

As described in the Homeland Security Advisory Council's Cyberskills Taskforce Report (2012), DHS has a critical need to train employees in ten mission-critical jobs (e.g. System and network penetration testing, Application penetration testing, Security monitoring and event analysis, etc.). According to a former senior DHS official, DHS has about 1,500 to 1,600 people in jobs requiring these cyber operations skills, many of whom are contractors. Required training for these jobs is highly specialized and technical, and developing a pipeline of prospective employees for such jobs is a challenge. One of the Taskforce's recommendations is that DHS should create a new Centers for Academic Excellence – Cyber Defense program focused on computer network defense, including secure provisioning of new systems and secure operations of existing systems. The recommended program would be developed using the approach developed by the NSA for the CAE – Cyber Operations program which built a higher standard inside the CAE program based on specific topics that courses needed to include and specific measures of skill mastery to ensure that graduates could actually do the jobs.

One specific area where DHS does possess the required infrastructure to conduct large-scale cyber security training is providing digital forensics training to law enforcement. The Federal Law Enforcement Training Center (FLETC) provides basic and advanced courses to DHS as well as state and local law enforcement officers. Approximately 1,000 people attend these courses each year. The curriculum includes: Digital Evidence Acquisition Specialist Training Program (DEASTP), Introduction to Digital Evidence Analysis (IDEA), Seized Computer Evidence Recovery Specialist Training Program (SCERS), Mobile Device Investigations Program (MDIP), Computer Network Investigation Training Program (CNITP) and the Macintosh Forensic Training Program (MFTP) (FLETC Journal, Summer, 2013, page 30). A second training facility, the National Computer Forensics Institute (NCFI) is operated by the US Secret Service in collaboration with the State of Alabama. The mandate of the NCFI is "to provide state and local law enforcement, legal and judicial professionals a free, comprehensive education on current cyber crime trends, investigative methods and prosecutorial challenges. Since its opening in 2008, the state-of-the-art facility has trained more than 2,400 state and local police officials, prosecutors, and judges from all 50 states and three U.S. territories." (see Beers, 2013).

The cyber security education and training resources for the millions of people in the Homeland Security Enterprise (HSE) is almost certainly worse than that for the DHS agencies. The HSE includes "DHS officials from all directorates, and components, officials from other federal agencies with homeland security responsibilities, members of relevant Congressional committees and subcommittees, State and local governments, nongovernmental entities, the private sector, interested communities, and concerned citizens" (Kahan, 2013). Some of the people may work at agencies that are large enough to support systematic training programs, but many HSE employees work at very small state and local agencies, some on a volunteer basis. Much of their

training is supported by grants, but funding is scarce and cyber security must compete with training required on other topics. It is extremely difficult to develop and deliver basic, let alone comprehensive, cyber security training to the majority of the HSE. Even large agencies such as the Port Authority of New York and New Jersey still only do minimal training, using canned online courses produced by private sector organizations such as Enterprise Training Solutions. In discussions with the Port Authority's Chief Information Security Officer, we learned that the initial training is handled through HR and it is not repeated. However, the Port Authority does subscribe to alerts from both State of New York and State of New Jersey homeland security cyber security experts, and these are shared with the workforce as appropriate.

3.2.2 US Military

As part of our research, the project team collected information about how the US military trains its officers and enlisted personnel in cyber security. While our analysis is by no means complete, we think it is important to know about the military's cyber security training for several reasons. First, for decades the military has been using sophisticated information systems, computer networks, and wireless networks and has been concerned with protecting those systems and networks. Recently, because of the rising threat of cyber war and the involvement of cyber activities in traditional ("kinetic") warfare, cyber security education and training has an even higher priority in the military. The US Cyber Command is headed by a very senior military officer who is also the Director of the NSA. Each of the major services has established a new organizational command under the US Cyber Command (the US Army Cyber Command, the US Fleet Cyber Command, and the 24th Air Force). Second, the US military has very mature training organizations and facilities, and tracks the training of its personnel throughout their careers. There may be lessons to be learned from the military by DHS and other organizations with less mature structures. However, as a former senior DHS official told us, there are substantial differences between the military which operates in a strategic, highly centralized, top-driven fashion, and the HSE which tends to operate in a tactical, distributed, and bottom-driven fashion. We should not expect that training in the HSE will mimic training in the military. Third, given the priority on cyber security education and training in the military, there may be lessons to be learned from military education institutions concerning cyber security curriculum development for universities and education and training techniques for DHS.

The information we have received from professors teaching cyber security at the three major military academies suggests that that these schools are among the leading institutions in implementing best practices for cyber security curricula. The US Military Academy, the US Naval Academy, and the US Air Force Academy have all received the NSA/DHS designation as Center of Academic Excellence for Information Assurance Education (CAE/IAE). An important aspect of their curricula is providing cyber security education to all students, not just computer

science majors or electrical engineering majors. For example, all cadets going through the US Air Force Academy take CS110 which includes the following cyber security topics: cryptography, authentication, cyber crime and ethics, forensics, phases of cyber attacks, cyber reconnaissance and vulnerability assessment, cyber attack, and cyber defense. Labs are included as part of this course. A second key course in cyber security, interestingly enough, is in political science. At the US Military Academy, all students take IT105, an introductory information technology course that includes computer security. The US Naval Academy requires all midshipmen to take two cyber security courses: SI 110 Introduction to Cyber Security for all first-year students, and EC 310 Applications of Cyber Engineering for all third-year students. The Air Force Academy offers a computer science major with a concentration in cyber warfare, which about 80% of the computer science majors complete. The US Military Academy recently added a Cyber Security minor in its Department of Electrical Engineering and Computer Science. The US Naval Academy began offering a Cyber Security major starting in 2013.

It is interesting to note that not all of the five Joint Professional Military Education (JPME) institutions, where senior military officers return later in their careers, are advanced at including information technology and cyber security in their curriculum. A recent Pell Center report (Spidalieri, 2013) notes that only two of the five institutions have received the CAE/IAE designation. Furthermore, a survey of the curricular offerings related to cyber security at each institution showed a wide disparity. Institutions demonstrating best practices in this area offered a robust set of core information technology courses, some of which focused directly on cyber security; they offered elective cyber security courses that could be taken by students pursuing different areas of concentration; they also offered the possibility of enrolling in cyber security courses at other universities, and provided seminars, conferences, and other training opportunities on cyber security.

The services have also established cyber security training programs and related career paths for enlisted personnel. For example, the Air Force now has about 250 enlisted cyber specialists and needs several hundred more (Kenyon, 2013). Its training program consists of an eight-week basic course followed by specific mission training and skills qualification depending on the airman's assignment. The Air Force also has implemented an extended training curriculum for enlisted and officers consisting of three levels of courses after initial assignment. The 200-level (to update existing skills and introduce new skills) courses are typically taken after six years of service, and 300-level courses (less focus on technology and more on joint cyber operations and strategic implications) after ten years. Enlisted people and officers often take the 200- and 300-level courses together. Courses at the 400-level are for lieutenant colonels and colonels and are focused on policy issues and refreshing skills. The courses are open to civilians working in cyber security for the Air Force, and to military and civilians from the other services.

Among military units, the National Guard is uniquely positioned to be able to provide cyber security expertise to both DoD and the individual states enabling it to provide cyber support to the wider HSE. In a recent interview, Col. David Collins, the chief cyber staffer at the National Guard Bureau, noted the key role that the Guard can play in cyber security, but stressed that this role is still being defined (see Freedberg, Jr., 2014). The potential advantages of the Guard include the fact that their distributed civilian employment often means that guardsmen are in contact with a number of civilian networks and their operators. The Guard can operate under orders from the federal government (Title 10 status), or under orders from a state governor (Title 32 status), and in the latter case can assist in law enforcement activities. Cyber security experts in the Guard also would likely have full time jobs in civilian information technology, which would give them a different and possibly deeper expertise compared to their active-duty counterparts. Collins described the Guard's current limited cyber security capability as "very ad hoc." Each state has authorization for an eight-soldier Army National Guard network security team, and the Air National Guard has network warfare and information warfare squadrons varying in size and skills. Yet, there is great potential for the National Guard to take a leadership role in cyber security if its best practices are emulated by other branches of the military and get passed along to the private sector and components of the HSE by Guardsmen working on cyber.

3.2.3 Private Sector

Cyber security education and training in the private sector depends on the size and business of the companies. Very large companies, particularly those focused on defense and intelligence work for the government, may have mature training organizations capable of developing a portfolio of cyber security courses internally. They can track employees as they work through introductory and refresher courses appropriate to their job and level in the company. Companies not big enough to have extensive training and HR departments often hire consulting companies or individual contractors to provide one or more courses. These courses may range from general cyber security awareness for all employees to much more technical courses for specialists. Alternatively, the companies may pay for cyber security specialists on staff to attend refresher courses or get training leading to a desirable certificate. Depending on the nature of a company's business, it may subscribe to alert services from the FBI or other agencies that provide case studies and analyses of recent cyber security attacks, and provide access to these alerts to the cyber security specialists.

We cover the difficult issues small businesses face in cyber security education and training in Section 4.2.3, where we suggest that small businesses are most vulnerable to cyber attacks, and have the fewest resources to defend against them.

3.3 Educating and Training the Cyber Security Pipeline

In 2011 NIST projected that 700,000 new cyber security professionals would be needed by the year 2015 for the public and private sectors in the United States alone. This large and urgent need has led to an analysis of the pipeline for educating new cyber security professionals, and initial results suggest that the pipeline may be very difficult to fill.

Raytheon commissioned a Zogby survey in 2013 of 1,000 people aged 18 to 26 ("The Raytheon Millenial Cybersecurity Survey") to understand the interest of this age group in pursuing a career in cyber security. 82% of respondents said that no high school teacher or guidance counselor ever mentioned the possibility of a career in cyber security, and less than 25% believed such a career would be interesting (35% of males and 14% of females). However, 86% of respondents felt it was important to increase awareness of cyber security programs in the workforce and in formal education. The survey also showed than many respondents had engaged in risky cyber security practices.

An obvious place to look for talented students potentially interested in pursuing cyber security careers is in high school computer science courses, but the present numbers are not encouraging (the following data has been compiled from several sources by Exploring Computer Science: http://www.exploringcs.org/resources/cs-statistics). The number of introductory computer science courses has decreased by 17% since 2005, and the number of Advanced Placement (AP) computer science courses has decreased by 33%. While there are just over 42,000 high schools in the United States, only a small fraction of them (2,100) were certified to teach AP computer science in 2011, and only 21,139 students actually took the AP computer science exam. The percentage of high school students taking STEM (Science, Technology Engineering, and Mathematics) courses has risen over the last 20 years for every STEM discipline except computer science where the percentage declined from 25% to 19%.

As a way to improve access to AP computer science courses, the company Amplify launched a free AP computer science Massively Open Online Course (MOOC) in September, 2013 (School CIO, 2013). The results will be worth tracking. Initially, 1265 students signed up for the MOOC, which is being taught by an experienced, well respected and successful high school AP computer science teacher. Students can log in and receive new lessons and assessments each week, and can submit homework, tests, and quizzes any time before the end of the two-semester course. In addition to these students, the Amplify MOOC Local program will be working with more than 300 schools in 30 states to sign up additional students whose progress the schools can track and monitor directly. The Local program also provides coaches for individual students who are trained by Amplify, and well as access to additional instructional materials. The Amplify MOOC Local is being offered free of charge for the first year.

Very recent data show that the number of students majoring in computer science at US universities has been trending upward for the last five years after a period of decline (Zweben, 2013). These data suggest that numbers enrolled in AP computer science courses in high school may not be a consistent predictor of the numbers of students who go on to major in computer science in college.

The number of women going into some STEM fields has been growing, and in fact in some fields such as the biosciences, there are more bachelor's degrees being awarded to women than to men. However, this is far from the case with computer science. In fact, the percentage of bachelor's degrees going to women in computer science, which had hit 30% in 1991, is now down to less than 20% according to a 2013 report by NSF: "Women, Minorities, and Persons with Disabilities in Science and Engineering." In that same report, we see that for Engineering, the percentage for women is also under 20% (and has never gone much above that.) If we are going to look for more people to go into cyber security, a natural place to start is to try to attract more women into the field.

Cyber security in particular is a male-dominated field. And in spite of the growing demand for cyber security professionals, and the shortage of such professionals, the percentage of women in this field is "alarmingly low," according to the background for the upcoming April 2014 conference on Women in Cybersecurity to be held in Nashville (http://www.csc.tntech.edu/wicys/). The goal of this NSF-sponsored conference is to raise awareness of the possibilities in and generate interest among students for careers in cyber security, with an emphasis on women.

3.3.1 Current and Proposed Approaches to Filling the Cyber Security Pipeline

Two approaches relevant to expanding the cyber security student pipeline are being pursued. The first seeks to revamp high school computer science courses to attract a larger, more diverse group of students into computer science which in turn could be expected to result in more students developing an interest in and pursuing cyber security. In 2009 the College Board in partnership with the NSF began to prototype the development of a new course titled "AP Computer Science: Principles" (see College Board: New Course and Exam). In 2013 the NSF awarded a four-year $5.2 Million grant to the College Board to fully developed and test this new course. The College Board is investing $1.5 Million toward the creation of teacher support materials and professional development, and $2.0 Million to develop a platform for online assessment (see College Board Press Release, June 13, 2013). This course is undergoing extensive piloting in high schools and colleges, the latter to make sure the course is appropriate for an introductory college computer science course leading to other computer science courses.

The effort to develop this course also includes the development and validation of performance-based assessment tasks, and a means of encouraging females and other underrepresented groups of students to take the course. The project is currently in the Phase II pilot stage in which 37 high schools and 11 colleges will use the course for three years, with the full course launch scheduled for the Fall of 2016 and the first AP exams given the following May. The new AP exams are being piloted in some sites. Additional support for developing curriculum related to cyber security has been available through capacity-building awards from the CyberCorps Scholarships for Service (SFS) program funded by the NSF. The NSF continues to fund cyber security education projects through its Secure and Trustworthy Cyberspace (SaTC) program. Recognizing their vital interest in cyber security, private sector information technology companies such as Intel have also sponsored curriculum development.

The second approach taken to expanding the pipeline of students heading toward cyber security careers is to offer incentives to students to pursue degrees related to cyber security. One example is the CyberCorps Scholarships for Service (SFS) program that funds tuition, books and other educational expenses while providing a yearly stipend to the student ($20,000 per year for undergraduates, $25,000 for masters students, and $30,000 per year for graduate students). Scholarships are funded through grants awarded by the NSF to participating institutions which must be NSA/DHS CAE designated or show the equivalence. Students must enroll at a participating institution, and they owe a year of service for each year of scholarship received. Students can meet their service obligation by working at a Federal, State, Local, or Tribal Government organization in a position related to cyber security. Students also must participate in internships at government agencies in the summers between the academic years for which they receive scholarships.

Results of the CyberCorps SFS program are promising. Fifty-one universities hold awards, half in engineering or computer science, others in MPA, Law, MBA, and Public Health, averaging 6-10 students in a yearly cohort. We have heard from more than one expert that The University of Tulsa runs an exemplary program with 140 students over the last 5 years, and has 2000 applicants a year. These same experts also have highlighted exemplary programs at Purdue, CMU, and UIUC. The NSA employs the most students coming from this program (32% of all graduates from 2002 to 2012), followed by the military (17% across the three services). DHS has attracted only 3% of the graduates. To date, 71% of the students have remained on their jobs after fulfilling their obligations.

3.4 Educating and Training Students Not in the Direct Pipeline

There are several reasons to provide cyber security education for all students, beyond just those considering cyber security as a profession. The first is simply to raise awareness of the

students about cyber security issues, as a complement to and extension of educating "The Public" (see following section). While educating "The Public" tends to be somewhat ad hoc and uneven, educating students a bit more formally can assure more organized and complete coverage of the most important cyber security topics appropriate to specific grade levels. A second reason to provide cyber security education to all students, is to seed other professions with people familiar with cyber security concepts. A great variety of professions beyond cyber security itself will need professionals with at least a basic understanding of cyber security. Professions as disparate as engineering, law, business, finance, public policy, international relations, and others encounter situations requiring knowledge of cyber security beyond what may be taught to "The Public." Students preparing for many different professions can benefit from cyber security modules, elective courses, or perhaps cyber security minors. A third reason for providing cyber security education for all students is to increase students' awareness of cyber security as a possible profession, perhaps in combination with another discipline. Ideally there will be pathways to the cyber security profession even for those students making career decisions relatively late in their undergraduate programs.

Means of reaching students outside the cyber security pipeline include short modules that can be injected into various courses (not just computer science or computer engineering), and development of elective courses in cyber security. At least one of the experts we interviewed suggested that high schools should consider modules focused on cyber security as additions to Advanced Placement courses not only in Computer Science (where enrollment may be low), but also in Mathematics and Statistics courses where there are growing numbers of high-performing students. These students may have the aptitude for studying cyber security in college either as a major or as a minor in combination with another discipline. Still others have suggested development of modules for much more elementary courses in a variety of disciplines including the social sciences, cognitive sciences, and management science. It is important to observe that a good education in cyber security, whether for general audiences or specialists, needs to be much broader than just an education in technical subjects. Intel sponsors the development of modules for various STEM topics including cyber security. Recent examples include modules developed for the Youth Stem Network in San Jose and Girls Stem Network in Silicon Valley. An important aspect of these projects is collaboration with the NSF for testing and evaluating the effectiveness of the modules, and collaboration with community organizations and families of the students.

At the college level, cyber security modules have been designed as drop-ins for a variety of technical and non-technical courses (see discussion in Section 4.1.3). The National Science Foundation has sponsored the development of "Security Injections" by Towson University (see Security Injections @ Towson). The injections follow a template consisting of background on the topic, lab or homework assignments, a security checklist consisting of a well-defined set of procedures for identifying the security issue, and discussion questions. Modules cover topics

such as buffer overflow, integer overflow, input validation, and risk analysis, and are geared as injects to Computer Science 1 and 2 courses.

Note that there are many modules being developed for specialists and for practical training, but the modules we have in mind include those for the general student.

With any new materials, testing and certification is critical. Such testing is best done by a formal evaluator with educational evaluation experience who interviews both teachers and students before and at several stages after the module is used. It is important to identify in advance those hypotheses the evaluator is testing or desirable outcomes that the module is designed to achieve. At CCICADA and at the Center for Discrete Mathematics and Theoretical Computer Science (DIMACS), which is where CCICADA sits and which was founded as a National Science Foundation "science and technology center," we test modules by bringing them into the classroom, have a professional evaluator with educational evaluation experience conduct teacher and student evaluations, and have the evaluator interview both teachers and students before and at several stages after the module is used. We ensure that changes are made in the module based on these evaluations and also based upon comments of subject matter experts and educational experts. We are strong believers in modules and in particular in modules that are tested and evaluated by both SMEs and educational experts.

Besides security modules, colleges offer introductory cyber security courses and cyber security electives. As noted above, the military academies require all first year students to take an introductory course that focuses on cyber security, no matter what major the student is pursuing. The academies also offer a number of cyber security electives that are open to other majors, e.g. cryptography, ethics, cyber law, cyber politics, cyber physical systems, etc. Some of these courses are multi-disciplinary in nature and can be taught by faculty in various departments.

Spidalieri (2013) analyzed the extent to which the top Master's-level graduate programs in business (MBA), Public Administration (MPA), Public Policy (MPP), International Relations (IR), Law (MLL), Criminal Justice, and Healthcare Management expose students to cyber security. She analyzed whether each school offered a core course in information technology that included a section on cyber security, whether similar elective courses were offered, whether students had the opportunity to enroll in elective information technology and cyber security courses offered in other departments, and whether occasional conferences or seminars on cyber security were given. Using a scale of 0 to 4 to compare programs, Spidalieri found that no program at any school scored a 4, while numerous schools offered programs scoring below 2, meaning that even top programs in these fields offered rather limited opportunities for their students to learn about cyber security. This is an area where work is needed to develop materials (modules being a prime candidate) to make these courses more relevant to cyber security.

In this section we have emphasized education for students in existing programs. However, contextual, on-the-job learning is a key component of cyber security and is centrally related to day to day operations in the cyber security role. This can be done through internships, cyber security warnings such as those provided by federal and state agencies, and regular training modules. More on this topic, especially on the importance of internships, is in Sections 4.1.2, 4.2.5 and 4.4.3.

3.5 Educating and Training The Public

Although most of this report focuses on cyber security education and training in formal educational settings, raising awareness of the public outside of those settings is also extremely important. Most people in the country are not currently involved in formal education and training, and yet virtually everyone needs basic awareness and some knowledge and rules about cyber security. Anyone using smart phones or personal computers for browsing, email, playing games, shopping, banking, paying bills, filing tax forms and an increasing number of other daily activities needs to know some basic information about cyber security threats, attacks, and consequences. Parents and guardians need to know how to convey this information to children. Everyone also needs to know at least some simple precautions and remedial actions they can take to protect against cyber attacks.

The National Cyber Security Alliance (NCSA) is a non-profit private-public partnership working with DHS on its mission "to educate and therefore empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individuals use, the networks they connect to, and our shared digital assets" (see http://www.staysafeonline.org/about-us/). The goal of the NCSA is to raise the awareness of cyber security to the level of other cultural messaging concerning good practices such as eating healthy and driving safely. Public awareness activities led by the NCSA include the promotion of National Cyber Security Awareness Month each October, the propagation of the "STOP. THINK. CONNECT." message, Data Privacy Day on January 28th, and the Re: Cyber program dedicated to business executives concerned with cyber security risk management. The NCSA also provides a wealth of information and cyber security tips for individuals, parental guidelines, K-12 instructional materials, and cyber security information for businesses.

Other organizations encourage and support their members to reach out to children and educate them about cyber security. For example, the Girl Scouts of the USA has partnered with DHS and joined the STOP. THINK. CONNECT. Campaign's National Network. Through this partnership and by using the Campaign's materials and toolkit, the Girl Scouts will be raising awareness of cyber security issues among its members. Guidance for girls includes sharing with care, protecting yourself while online, protecting your information, protecting your computer,

and cyberbullying (http://forgirls.girlscouts.org/internet-safety/) Another example is the International Information Systems Security Certification Consortium (ISC)2. This not-for-profit organization mainly exists to provide certification and training in various areas of cyber security. However, it encourages its members to educate children about cyber security through its "Safe and Secure Online" program. The program supports these volunteers with age-appropriate instructional materials, tips about educating children, connections with schools, etc. Since 2006, more than 800 (ISC)2 members have educated close to 100,000 children aged 7 – 14 about cyber security. As described in Section 4.2.1, Microsoft, through the Microsoft Safety Center, also provides age-appropriate guidance and tips for educating children about cyber security.

An example of another approach to educating the public is the America's CryptoKids website (http://www.nsa.gov/kids/home.shtml) for future codemakers and codebreakers. The site is sponsored by the NSA and clearly is focused on raising the awareness of grade-school and high-school aged children about cryptography and possible careers involving cryptography at the NSA. The site includes games and activities, brain teaser topics, codes and ciphers, an online museum, and student resources. In the resources section, students can find out about careers related to cyber security, high school and college programs, cryptologic events, etc.

While there are numerous resources available to educate the public regarding cyber security, it is not clear how many people are being served by them, how complete they are, or how effective are the different modes of delivering this education.

3.6. Coordination: NCCIC

Within DHS, the National Cybersecurity & Communications Integration Center (NCCIC), which is within the Office of Cybersecurity and Communications, has a critical role in coordinating information about evolving cyber security threats and responses. NCCIC partners include all federal departments and agencies. As referenced previously, the US Computer Emergency Readiness Team (US-CERT), a component of NCCIC, receives reports of all incidents of cyber attacks against federal agencies. We heard from a variety of people about the importance of this incident reporting. Beyond the connection with all federal agencies, the NCCIC also has as partners, all state, local, tribal, and territorial governments, the private sector, and even international entities.

The NCCIC mission is "To operate at the intersection of the private sector, civilian, law enforcement, intelligence, and defense communities, applying unique analytic perspectives, ensuring shared situational awareness, and orchestrating synchronized response efforts while protecting the Constitutional and privacy rights of Americans in both the cybersecurity and communications domains" (see https://www.dhs.gov/about-national-cybersecurity-communications-integration-center).

The NCCIC gathers information about cyber attacks, responses, vulnerabilities, etc. from its diverse set of partners. It has the expert staff and technology to analyze that information and develop mitigation responses to cyber attacks. The NCCIC also shares its analyses and responses with its partners in real time. In this way, the NCCIC can provide a widely shared situational awareness about cyber threats, and enable a coordinated response by many public and private entities – essentially the entire nation.

An important role of the NCCIC is to serve as liaison to the Information Sharing and Analysis Centers (ISACs). The ISACs have been established by owners and operators of critical infrastructure and key resources (CI/KR) for different sectors (the National Council of ISACs includes 17 different members including Financial Services, Maritime, Supply Chain, Transportation, Communications, Oil and Natural Gas, etc.) to provide all-hazards analysis shared within the sector, across sectors, and with the government. ISAC services include risk mitigation, incident response, alerts, and information sharing. During events of national importance, the NCCIC can provide emergency classified briefings to ISAC members, and sector threat reporting. Through the NCCIC and its role with the ISACs, DHS is in position to provide the private sector as well as state and local governments with timely education and training on cyber security threats and responses.

4. Observations on Four Clusters of Questions

We have identified several clusters of questions based on information from the brainstorming workshop, literature search, and the email surveys and phone interviews. These questions, and the further information required to complete their answers, form the basis for the report's recommendations.

The clusters are:

- Questions concerning the implications of the evolving nature of cyber security threats and responses
- Questions concerning cyber security education/training approaches in different communities and organizations
- Questions concerning principles of teaching and learning applicable to cyber security education/training
- Questions concerning the effectiveness of cyber security education/training

These clusters are more fully described in the following.

4.1 Implications of the Evolving Nature of Cyber Security

Questions related to the implications of the evolving nature of cyber security threats and response include:

- How does the constantly evolving nature of cyber security threats and responses, as well as the rapid evolution of the devices to which these threats and responses relate, change what is taught?
- What can we learn from analogies with other disciplines that face constantly changing challenges?
- How do cyber security research results make their way into education and training materials?

4.1.1 Educating for Constantly Changing Cyber Security Challenges

Students, whether those specifically preparing for a career in the cyber security workforce, or those enhancing their education in another discipline with cyber security courses, should understand the evolving nature of cyber security threats and responses. They need to understand that they cannot simply acquire a static body of knowledge in school and expect that their cyber security education is complete. Even those students – and the public – who are not specializing

in cyber security to the extent of taking a course in the subject should understand the evolving nature of cyber security threats and responses. For them, a key is to develop fundamental principles of cyber security that will withstand the changing landscape.

The changing nature of cyber security threats stems from several sources. The high rate of change in software applications, operating systems, and web sites continually opens new vulnerabilities as demonstrated by the rate at which new security patches arrive. New kinds of hardware, including end user devices, new computers, networking gear, etc. may introduce new kinds of vulnerabilities. Cyber attackers' strategies evolve and become ever more sophisticated. New groups of cyber attackers have different motivations (political, financial, national security, etc.) meaning that different targets become desirable. A component of cyber security education should include an analysis of these and other factors that underlie cyber security threat and response evolution.

To address changing cyber security challenges, the cyber security curriculum should include general principles that are likely to have enduring value and do not change as quickly as the evolving threats and responses. One place to find such principles is in the best information security textbooks. These principles include but are not limited to:

- The CIA (confidentiality, integrity, availability) model
- Identification and authentication, authorization and access control
- Auditing and accountability
- Basic concepts of cryptography
- Policy development and enforcement

The experts we talked to have different opinions about these principles. For example, one expert recommended starting with the ISC2 body of knowledge instead of the CIA model. Different people we talked to differed on whether there were new principles that arise because of evolving devices, threats, and responses. A more detailed study than ours should aim at addressing this question.

Ways to introduce these principles need to be developed. However, these ways will differ depending upon whether those being targeted are cyber security experts (or future experts) or others, and also upon age level, prior exposure to relevant technical topics, etc. To some extent this is a matter of level of detail, frequency of repetition of the principles, etc.

Beyond such general principles, cyber security students aiming at becoming specialists should be exposed to and learn how to incorporate information from "just in time" training resources. These include cyber security alert services, reports on recent cyber security case studies, relevant conferences, tutorials, and workshops, and online training resources. In Section 4.4.1, we note that one measure of effectiveness of a cyber security education program is the extent to which those training to become cyber security experts attend such conferences, tutorials and workshops

and make use of online training resources. Part of the evaluation of cyber security students could include how well they make use of these resources. It is important for students entering the cyber security workforce that they expect to continue using these kinds of resources on the job.

Sharing information and "best practices" is a good way to keep up with evolving challenges. This is especially relevant to "on the job learning" and "adaptive learning" that addresses how today's subject matter expert in one discipline needs to be a life-long learner to keep up with new disciplines and rapidly changing contexts in which to apply the discipline in which they were trained. DHS could play a major role here, for example in enhancing already-existing approaches to information sharing by developing updates and best practices guides both for new approaches to cyber defense and to education/training, to be shared across its components, with the Homeland Security Enterprise, and also with the private sector. Enhanced methods to share in the reverse direction would also be very useful. All of this is very relevant to day to day operations of cyber security departments.

The changing nature of threats and attacks is especially complicated since in the case of cyber security, a given type of attack might peak rapidly in terms of frequency but then diminish at first rapidly and then gradually. Still, the threat remains – there is a long tail in the graph of time vs. frequency of appearance of each type of attack. The implications of this are that cyber security expects need to be fast learners – they need to understand new threats quickly – but they also need to retain knowledge of threats for a long period of time. This also has implications for how we educate and train cyber security experts, e.g., through the use of fast "current threat" alerts but also through repetition and reminder of past threats that are not quite gone.

4.1.2. Analogies with Education and Training in Other Disciplines Facing Evolving Challenges

In thinking about how cyber security education and training should address the constantly evolving cyber security threats and responses, it might be helpful to consider analogies to education in other disciplines facing similar challenges. Such analogies will also be helpful with other questions we are addressing, though in this report we emphasize the usefulness of such analogies in the context of evolving challenges. While no analogy is perfect, here are some of the characteristics of cyber security education and training that could be included in an appropriately analogous situation.

- The education and training should allow for specialties. The NIST/NICE Framework identifies thirty-one cyber security specialties.
- The education and training should include a role for internships. We have heard from our interviews that successful cyber security educational programs include practical internships. However, because of budget cuts, internships in cyber security are becoming harder to find.

- The education and training should include team problem solving, particularly by multi-disciplinary teams. We have heard about the importance of cyber security students learning to work in team settings, taking on different roles, and working with non-technical team members.
- The education and training should include preparation for situations not previously encountered or even envisioned.
- The education and training should have a continuing component beyond the terminal degree. Participation in professional associations that promote long-term internalization of professional standards and codes of ethics should be encouraged. Such organizations also publish journals, and run workshops and tutorials. Note, that while we view continuing education in cyber security as crucial, we are not proposing that a professional certification program is appropriate at this time -- see findings of the National Academy of Science Professionalization Project. However, in line with the NAS report, perhaps more options for certification could be explored, especially subfields identified that are closer to ready. The report explicitly says that digital forensics is an area that is sufficiently coherent already and as such could move forward with certification.

Given these characteristics, analogies with education in several other disciplines are worth exploring. In this section, we discuss medical education, emergency medical education, public health education, engineering, and business. We also reiterate some of our comments about Military Education made in Section 3.2.2.

Military Education: Military education is discussed in Section 3.2.2. It is worth repeating the following observation made in that section. There may be lessons to be learned from the military by DHS and other organizations with less mature structures. However, as a former senior DHS official told us, there are substantial differences between the military which operates in a strategic, highly centralized, top-driven fashion, and the HSE which tends to operate in a tactical, distributed, and bottom-driven fashion. We should not expect that training in the HSE will mimic training in the military. One way in which we might benefit from the military's training is the distinction the military makes between deliberative, advance planning, and crisis planning. Planning for cyber security or cyber defense also takes these two forms and it is important as we develop cyber security education and training programs to emphasize the distinction between these two types of planning and to develop programs that prepare cyber security experts to develop, modify, and implement the two types of plans.

Medical Education: Medical education analogies apply to preparation of cyber security professionals. Medical education involves preparation for a large number of different possibilities. In this sense, this is analogous to cyber security education. There is no one topic or one course that can prepare professionals for all they may confront. Similarly, there is the need to prepare both medical doctors and cyber security specialists in a large number of topics. We know

that medical education requires practical experiences and an internship experience. Regarding team training, in medicine, while there are some situations where teams with multiple specialties are needed, not all medical doctors will necessarily work in team situations – though they certainly need to understand what specialists of various kinds have to say. Both medical doctors and cyber security specialists need to be trained in general principles of their profession, principles that will allow them to deal with situations they have not encountered before or even envisioned.

Medical education also involves some type of certification, i.e., licensing. However, as noted in Section 3.1.4, because of the anticipated serious shortage of cyber security professionals, we might not want to make certification mandatory in the short run, for fear that it would deter some people from entering the profession. Perhaps "Board Certification" is a better analogy – this certifies those who have achieved a certain level of expertise beyond just the basics. The example of subfields such as forensics being potentially ready for this kind of advanced certification is relevant here. The question arose during our discussion as to whether medical licenses or certifications require examination for renewal – and this needs to be studied and analogies described to potential procedures for cyber security experts. Certainly both medical doctors and cyber security specialists need lifelong learning, and how this is accomplished through exams or practical experiences or other training is another area for potential analogies.

Medical education increasingly exploits new technologies in ways that may also be useful in cyber security education. One such technology is simulation which in medical education can include virtual reality simulators, high-fidelity mannequins, task trainers, etc. The analogy for cyber security education would be simulated or self-contained networks and systems where students could study, probe, perform "lab exercises," respond to staged attacks etc. without doing damage to a live system. Another technology adopted in medical education is distance learning, which may be used in certificate programs and degree programs. MOOCs are one form of distance learning already being tried in cyber security education. These and other forms of distance learning should be explored when access to SMEs or simulations may be limited, or when distributed team training is desirable. Learning management systems are a third kind of technology used by medical education. These can enable information sharing across organizations, and provide learning diagnostics, analytics, and feedback to improve the learning process.

Emergency Medical Education: Education of EMTs: The training of EMTs, and more generally of first responders and those working with Hazmats, also has useful analogies for cyber security education. For EMTs, practical experience is essential. EMTs work on teams and are trained to do so. A new EMT would not/should not go out alone. In effect, they intern while learning their job. Also, there are levels of certification for EMTs that allow them to do different things. For instance, you can be certified to drive, but not to lead a team. Standards for what one is allowed

to do are nationally consistent. It is important to note that there is a difference between expertise and awareness. For example, everyone (including non-EMTs) should be aware of Hazmats and that you should avoid them. But only those trained to work with them should get involved. Note: Regular retraining is necessary too.

Public Health Education: There are good analogies with what we teach "the public" and what we teach children in grades K through 12. In public health, we teach basic practices that promote good public health: wash your hands regularly, sneeze into your sleeve, stay home if you are running a fever, etc. We then move to more advanced concepts, such as how to protect yourself from sexually transmitted diseases and how to prevent pregnancy. In cyber security education, we want children and young adults to learn a few "good health" practices, such as not to open an attachment when you don't know the source, not to share private information, how to keep passwords safe. More sophisticated tools can come later.

The analogy with public health education also applies to educating public health professionals. Certainly there are many public health career specialties, as there are in cyber security. Public health internships are regarded as a key component of training public health professionals. The US Public Health Service (USPHS) has an extensive team structure in which Applied Public Health Teams (APHT) are organized into nine mini-teams of specific expertise (e.g. epidemiology, preventive medical services, environmental public health). Public health professionals also need to maintain their certification through continuing education.

Engineering: Many aspects of educating and training engineers, specifically civil engineers, may be good analogies for cyber security. Engineers must be trained to deal with problems they have not seen before. Engineering training is flexible in that it places an emphasis on basic principles that can be applied to a broad range of problems. Therefore, when confronted with a new structural engineering problem they can solve problems using basic principals about structural design and the behavior of materials. Teamwork is essential for engineering students because most major projects are accomplished by cross-disciplinary teams. Group projects are often assigned so that students get experience coordinating their work with others. Internships are used extensively in Engineering. They provide a good introduction to what practice is really like. Many students arrange internships on their own, but there are also organized programs. For example, the New Jersey construction industry funds 10-12 internships per year for Civil Engineering students to promote interest in careers in construction. The engineering community also has developed means for sharing information about emerging threats and new approaches. For example, the American Society of Civil Engineers provides considerable coverage of emerging problems and threats through their magazine and web pages. Considerable coverage is now given to global warming and rising sea water levels.

Recent practices in the civil engineering profession may provide useful analogies to cyber security in certification and continuing education. In engineering training there has been an increasing use of certification to identify individuals with specialized credentials. In particular, the LEED program certifies individuals as having knowledge of the most current green building principles and practices. LEED is a building rating system promulgated by the U.S. Green Building Council. Building projects can be rated according to their sustainability. For building construction LEED is the most highly used green standard. An engineer or architect who has been certified as a LEED associate has the expertise to design and build sustainable buildings that can then be highly rated according to the LEED standards. To be certified as a LEED associate requires a student to take a training course and to pass a 100-question exam. More experienced personnel can be certified as a LEED Fellow. Perhaps an equivalent scheme could be developed to certify an individual as having knowledge of the basics of a cyber security specialty. Other, more advanced certifications could be developed for personnel with more extensive knowledge and experience in that specialty area. A topic for further research would be to identify specialty areas or clusters for certification, and determine which ones are mature enough for certification programs.

Another well known certification program is run by the Project Management Institute (PMI). Because civil construction is done of a project basis, many people in the construction industry seek this certification. PMI offers six credentials that are obtained through training courses and passing an examination. What is interesting about PMI's program is that it provides various levels of certification, as well as providing specialist certification. For example it is possible to be certified as a scheduling professional. A scheme like this has considerable applicability to cyber security where a computer novice could be certified as understanding basic security measures, whereas an IT professional could be certified as having advanced skills to protect businesses computers and networks.

The continuing education model in engineering might also be a useful analogy for cyber security. In some engineering disciplines, an engineer with a B.S. degree can become licensed as a Professional Engineer. After taking an initial exam when graduating from college, and garnering four years of experience an engineer can sit for the Professional Engineer exam. Because of rapid advances in technology, many states now require licensed engineers to prove that they have taken training in new methods to maintain their license in an active state. These states require a licensed engineer to accumulate a certain number of Continuing Education Units (CEUs) to certify that they are familiar with the most recent engineering knowledge. Generally, a CEU is defined as ten hours of participation in a recognized continuing education program, with qualified lecturers and sponsorship. In engineering many seminars and courses qualify to grant CEUs. This is a technique that could be employed in cyber security education. With cyber threats constantly changing, a CEU program could insure that already certified personnel are kept up to date with the latest developments

Business Education: While we have not studied Business Education very extensively, one relevant analogy to cyber security may be accounting. A CPA must understand the implications of law and ethics, both of which apply to cyber security. The notion of certification comes up in accounting, just as it does for medicine and for cyber security. Indeed, a CPA needs to go through an increasingly rigorous set of stages of certification and yearly mini-course requirements – again a model we might want to consider for a cyber security specialist. The evolving challenges in accounting have to do with changes in federal and state laws, changes in the tax code, changes in accounting practice, and new accounting tools and systems. The role of follow-on courses, accounting specialties, internships, and team problem solving in accounting education needs to be examined to determine whether there are more useful analogies for cyber security education.

4.1.3 How do Cyber Security Research Results Influence Education and Training?

An important problem for any discipline that has a rapidly evolving research base as well as urgent needs for applied solutions is how to transition research results into the hands of practitioners as efficiently as possible. While a number of interviews and presentations have pointed out this problem in cyber security, we have not discovered any definitive solutions.

How do cyber security research results make their way into educational/training practice? This issue is probably most important for two target student groups: the existing cyber security workforce, and students in the cyber security pipeline. For students in the workforce, there are examples of presentations by academic researchers geared toward practitioners. The annual International Conference on Cyber Security (ICCS) is one example of a conference that specifically fosters the transition of results from academic researchers to the cyber security workforce in government agencies and industry. There are other examples, of course, e.g., the ISSA conference, the ACM CCS conference, the annual RSA conferences, Blackhat, DefCon, etc. ranging from peer-reviewed research presentations to hacker demonstrations. Courses on aspects of cyber security may be presented by academic researchers through companies such as Microstrategy, Inc. that market to the cyber security workforce. It is easy to imagine that blogs and online courses aimed at the cyber security workforce might also be vehicles for transitioning the latest research results.

Two projects at the CCICADA Center are focused on getting the very latest cyber security information to people encountering new cyber security threats. The Personal Security Assistant helps users to understand security issues and customize off-the-shelf security tools. The approach is based on semi-automatically learning the user needs and best security practices, and then using this knowledge to assist the user with security decisions. The Assistant adapts to the

changing environment and evolving user needs by observing the user behavior and asking targeted questions, adapted to the level of the user's knowledge. This allows users of iPads and smartphones, as well as users of social media such as FaceBook and Twitter, to have personalized learning/training related to their devices and the way they use them. As new research allows Recommender Systems to become more and more sophisticated, we can expect such personalized learning/training to be expanded to all kinds of contexts, whether for unsophisticated or sophisticated users. Research on the confluence between mobile devices and the cloud is another area that can influence personalized learning. So is research on detection of cross-site forgeries, document similarity to detect web attacks, biometrics for botnet detection, trustworthiness of online sources, and crowdsourcing for threat detection.

A second CCICADA project, Personal Cyber Security Assistant / Smart Notes, improves defenses against threats targeting careless or naïve users of devices. It uses crowd-sourced information and applies machine learning and natural language processing to analyze messages and reports from cyber attack victims, to identify system behaviors, harm caused, and applied remedies. The project is working towards the automated interpretation and classification of newly reported threats into a portal that supports user questions for remedies, requests for further information, software to automatically classify incoming emails, webpages, documents, and possibly software as to whether it is malware or not, and the detection of cyber attacks by their observed symptoms as expressed by users on public online forums.

It may be a more difficult and lengthy process for cyber security research results to make their way into more traditional educational materials like textbooks and problem sets for students in the cyber security pipeline. We need ways for researchers, educators, and possibly other stakeholders to work together to determine which research results are relevant for which educational/training contexts, and how to adapt and disseminate them to appropriate educational/training contexts. All this must be accomplished in a very timely fashion. A possible complement to this process is for academic researchers to include new research results in updates of their online course offerings including Massively Open Online Courses (MOOCs). Another approach is to develop "modules" that can be inserted for short periods such as a day to a week in an existing course. DIMACS and CCICADA have found considerable success in developing such modules for education in bio-mathematics, sustainability, and computational thinking, at levels from high school through advanced undergraduate. The SEED project at Syracuse has developed an instructional lab environment and lab exercises that can be used as adjuncts to computer science courses (see http://www.cis.syr.edu/~wedu/seed/). The "security injections" developed at Towson University are examples of strategically placed computer security-related modules for existing undergraduate classes. Modules can be developed for specialized topics and for specialized courses, and they can be inserted in many nontechnical courses as well. Indeed, Intel is now offering grants for development of modules on cyber security for a wide range of classes.

4.2 Cyber Security Education in Different Communities and Organizations

Aside from attempts to disseminate cyber security education to "the public," some of which may take place outside of specific organizations, cyber security education most often will take place within a specific community or organization. The community may be a child's family, the Boy Scouts or Girl Scouts, a grade school or university. Organizations providing cyber security education include government agencies and private sector businesses. Questions related to cyber security in these different settings include:

- At what age should we start cyber security education?
- What differences and what commonalities are there for cyber security education and training for employees in DHS, other government agencies, and the private sector?
- Does what works in a small organization generalize to a larger one and vice versa?
- At the college/university level, how does cyber security education for general university students relate to the education for students in the cyber security pipeline?
- What are key components of a successful cyber security education program?

4.2.1 When to Start Cyber Security Education

Children at earlier and earlier ages are using computers and smart phones to do a variety of things. As some people we have interviewed suggested, that does not mean we should start cyber security education as young as preschool. As people have found, teaching even simple things like "a car can hit you if you cross the road" to preschoolers is virtually impossible. Children at this age are interested in self-gratification first and foremost. For example, two and three year olds probably do not know what a stranger is or who's harmless and who's not. While you can begin to teach them basic safety, they're not ready for conversations about how to deal with strangers. By the age of four, many preschoolers have heard about strangers and you can start teaching how to stay safe. However, many children remain too young to be left unsupervised in public because they don't have good judgment or impulse control yet. The same can be said for safety on the Internet and strangers through the Internet. However, not everyone agrees that children even at age two or three or four cannot learn from exposure to some principles of cyber security. Indeed, as the Microsoft Safety Center points out, it is never too early to talk with children about computers. We also heard about some attempts to develop games that would expose nursery school age children to cyber security concepts.

Children in elementary school are not much different than preschoolers in their level of maturity needed for such complex understandings and cyber security, but the older they get, the more they can and should be exposed to some general principles such as those listed in Section 4.1.1.

By the teen-age years, children have the maturity to understand safety issues with using the Internet (Schaffhauser, 2008; Thomas, 2009). Some relevant data on teens:

- Children who are educated in the importance of online safety are more likely to take steps to keep themselves safe online than children who aren't educated.
- One out of five teenagers use their cell phones to go online. Of those who do, one out of five say their parents don't know that they do this.
- One half of all teenagers post their real age on social networking sites. Two out of five post the name of the city where they live.
- While 25 percent of 13- to 15-year-olds think it's unsafe to post personal stuff online, only 14 percent of 16- to 18-year-olds feel the same way.
- Two out of five teenagers are exposed to pornography online.
- Two out of three teenagers say that cyberbullying is a serious problem. One out of three say that online bullying is worse than being bullied in person.

More than one of the experts we interviewed suggested that middle school may be the "sweet spot" for introducing cyber security concepts into the classroom, including content designed to make children aware of possible careers in computer science and cyber security in particular. The thought is that by high school, children are too distracted by competing academic (and other) demands, and that it is in middle school when children begin to form opinions about what they are good at.

The Boy Scouts of America Cyber Chip program provides a useful model for educating children about cyber security. It specifies age-specific requirements that must be renewed each year in order to wear the cyber chip badge. Sets of requirements span grades 1 to 3 up to grades 9 to 12. Topics include cyberbullying, cell phone use, texting, blogging, gaming, and identity theft. Instruction is delivered via short videos, games, group activities, and discussions with parents and scout leaders. These are good examples of what educational theorists call "learning progressions," and are discussed more in Section 4.4.3.

The Microsoft Safety Center suggests a number tips for keeping children safe, related to age level (see http://www.microsoft.com/security/family-safety/childsafety-age.aspx). The following gives an overview for each of the age groups considered. The site lists many detailed suggestions for each age group.

For children up to the age of 10, strong parental supervision is suggested, including sitting with children whenever they are access the Internet.

While children aged 11-14 are savvier about their Internet experience, it is sill recommended to supervise and monitor their Internet use to help ensure they are not exposed to inappropriate materials. Internet safety tools can be used to limit access to content and websites and provide a

report of Internet activities. Children in this age range must understand what personal information they should not give over the Internet.

Teens 15 to 18 should have almost limitless access to content, websites, or activities. They are savvy about the Internet but they still need parents to remind them of appropriate safety guidelines. Parents should be available to help their teens understand inappropriate messages, avoid unsafe situations, and to remind teens what personal information should not be given over the Internet.

4.2.2 Cyber Security Education and Training in DHS, Other Government Agencies, and the Private Sector

When considering how to educate/train employees in various organizations about cyber security, it is important to take into consideration the specific mission of the organization as well as the role of the employees to be educated or trained. For example, it is not likely that a single approach to cyber security training and education would work for the Department of Homeland Security, since its 22 constituent agencies have quite different missions, and its 240,000 employees span a huge range of cyber security responsibilities. It is obvious that an employee monitoring networks at the NCCIC needs different cyber security training than an employee operating a warehouse for FEMA, who in turn would need different training than a TSA employee checking passenger credentials. Other government agencies and private sector companies present a similar range of missions and job responsibilities. It is fair to say, then, that there will be rather large differences in education/training goals and methods depending upon which DHS employees are being considered. The wide variety of needs is even greater if the extensive homeland security enterprise is considered. Another important point to consider is that priorities for cyber security education and training will have to differ depending upon the time horizon that is important. In the short run, one may have to depend upon "quick fixes" in terms of education/training both for cyber security experts and the general DHS workforce. However, in the medium and long term, it seems very important to concentrate on the entire pipeline of future workers, and so not to separate education/training of the DHS workforce from education/training in colleges and universities.

In an interview with project team members, a former very senior DHS official distinguished several high-level categories of jobs for the purpose of tailoring cyber security education. So-called "cyber ninjas" or the "skilled pilots" are the 1,500 to 1,600 people in jobs requiring one or more of the approximately 10 mission critical skills described earlier (see Section 3.2.1). These people require really highly specialized training and need to stay on top of the constantly evolving threats and responses. A second set of people, e.g. electrical engineers working on the power grid, chemical engineers, gas and oil engineers, etc. also need specialized training,

although not to the level of the people performing the mission critical skills. Similar to the way that every police patrolman needs to be trained to respond to an active shooter now, this second group of people will be the first responders for many cyber security attacks on critical infrastructure and key resources, and must be trained to deter, detect, defend and mitigate such attacks. A third group of people are the IT professionals, including most of the jobs in the NICE Framework. These people need training to understand and implement a relatively small number of protective policies and procedures that can prevent 80% of attacks. As few as perhaps a half-dozen preventive measures can deter the attacks seen with the greatest frequency. More rare attacks will probably be best handled by a smaller group of people highly trained and constantly updated on the mission critical skills. Finally, there is everybody else, including grade school, middle school, high school students and The Public. For this very broad-based educational effort the former DHS official suggested an approach to cyber security education that is appropriate to the age or developmental level of the person to be trained.

The military makes extensive use of training games for exposing both generalists and specialists to problems they will face in the cyber world. Here too there are greatly varying goals and methods depending upon which military personnel are involved. It is certainly going to be useful to identify analogous jobs between the DHS and DoD personnel, as a way of helping to design cyber security education/training programs within DHS.

Some companies we learned about have also developed extensive cyber security education programs for both specialists and general employees. Very interesting examples are Raytheon, Honeywell, Associated Press, Microsoft, and Turner Construction. Just as between DHS and DoD, we should be able to identify analogies between jobs in DHS and jobs in the private sector that require somewhat similar training.

When developing cyber security education and training for an organization, consideration of the organization's mission should include what adversaries may want to accomplish via a cyber attack. Some organizations may present an attractive target for data exfiltration. For government agencies the data could include organization charts, plans, programs, and other classified or sensitive information, budgets, employee information, etc. Private sector concerns include intellectual property, customer data, building plans, corporate marketing and other plans, etc. Agencies and corporations, particularly those maintaining transactional web sites, may have exposure to disruption of their operations via cyber attacks. Others may be exposed to havoc caused by hackers injecting false news or misleading directions on informational web sites. Each organization will have different information sharing requirements and criteria, and different levels of emphasis on privacy.

Once an organization's cyber attack targets are understood, cyber security training can be provided to its employees to deter, detect, defend, and mitigate attacks. The training should be

appropriate for an employee's job responsibilities in the organization. Some employees may need awareness training, an extension of what the general public receives on such things as phishing attacks, and identity theft, but focused on how an adversary may use such attacks to threaten the employee's agency or corporation. Employees responsible for maintaining sensitive information may need more technical training on processes and tools to secure the information. Employees responsible for networks, operational systems, and hardware may require additional training on detecting, defending, and mitigating attacks against those components.

The cyber security education and training developed for different organizations should be sensitive to the different cultures operating across agencies and corporations. People in the military or a law enforcement organization may have quite different expectations regarding issues such as privacy, protocols, and compliance compared to people at a university or private company. However, both groups require cyber security education/training on an ongoing basis. The culture of the workplace can affect both the cyber security education and training process, as well as the cyber security policies and protocols deployable in the organization.

4.2.3 Does What Works in a Smaller Organization Generalize to a Larger Organization and Vice Versa?

Experts we have interviewed say that compared to large organizations, a small organization (e.g. a small business, a small government agency, a non-profit) is less likely to employ cyber security specialists, or have the budget for a robust cyber security education and training program. Typically the people responsible for systems and networks in a small organization wear many hats and cyber security is not their main concern. Their training tends to be informal, and done on their own time as compared to a larger organization where training is commonly a budgeted item and can be designed for and delivered to different groups of employees on company or agency time.

Cyber security threats against small organizations, specifically small businesses, are a major concern, partly because "the 'bad actors' and criminals on the Internet realize that small businesses often don't take many of the basic steps, making them more vulnerable because there is less rigor associated with the protection, monitoring, and maintenance of their networks, servers and workstations" (Small Business Cyber Security Guide, University of Southern Maine, October, 2013). Verizon's 2012 Data Breach Investigation Report showed that 72% of the data breaches they examined occurred in businesses with 100 or fewer employees. While in absolute terms the dollar value of a small business loss due to a cyber security attack may not be huge, it may still be devastating for a small business. Somewhat similar issues arise for smaller (e.g., local) agencies in the homeland security enterprise, which may not have the resources to hire dedicated cyber security specialists or devote much time to training employees. While agencies we talked to such as the New Jersey Office of Homeland Security and Preparedness have

extensive cyber security training and education programs, small health departments – to give just one example – may not.

While structured cyber security education and training delivered on site is likely to work for larger organizations, small organizations may benefit more from "self-help" style resources. One such example is the "Internet Security Essentials for Business 2.0" published by the U.S. Chamber of Commerce. Another is the previously referenced Small Business Cyber Security Guide from the University of Southern Maine. A third is the FCC's website "Cybersecurity for Small Business." These and similar publications and web sites are cognizant of the time demands and budget restrictions on employees in small organizations. They provide simple recommendations for implementing inexpensive practices to improve the security of information, computer systems, and networks.

4.2.4 At the College/University Level, how does Cyber Security Education for General College/University Students Relate to the Education for Students in the Cyber Security Pipeline?

At the university level, it may be useful to consider three categories of people we want to expose to cyber security: general university students; students interested in majoring in computer science or information technology, but not necessarily interested in becoming specialists in cyber security; and those who aim to become specialists, i.e., to make cyber security a career. We may ask whether training for the first group relates to that for the second group and that for the second group relates to that for the third group. For example, education for the second group might provide a gateway for the third group. Given limited resources at universities or colleges or community colleges, we may need to emphasize relationships among these three groups in order to minimize number of courses and tracks toward a degree. This could be a major area of research in the future into good modes of cyber security education.

The general college/university students might be best served by an introductory course in cyber security with few if any prerequisites, and perhaps by a sample of elective courses (e.g. data security, social networking, computer forensics) with only the introductory course as a prerequisite. Indeed it has been suggested by some cyber security experts that a computing course including cyber security might become part of the general education requirements. But this may only be possible in an "ideal" world where we can devote significant educational hours to cyber security. Indeed, it is probably much more realistic to develop examples or "modules" (see earlier discussion) that can be introduced into other courses and that illustrate principles of cyber security. Such modules could be introduced into courses ranging from basic science courses to philosophy or business or environmental protection. Since returning to cyber security ideas from time to time is a good idea for everyone (see the principles of teaching and learning discussion below), we should think in terms of sequences of courses in a variety of majors, with modules in each course in natural sequences students take. Because it is never too late to capture

budding interest in specializing in cyber security, ideally, the curriculum for the second and third categories of students as defined above could be set up so that students could make fairly late decisions about switching into a cyber security concentration with a number of different majors.

A cyber security concentration might indeed be possible to complete under a number of different majors. Perhaps the most obvious major for cyber security is Computer Science. Our interviews have also suggested that majors in Statistics, Mathematics, Electrical Engineering, Communication and other disciplines can form a good foundation for a career in cyber security. However, as we have noted earlier, students need non-major courses (or at least background) in economics, political science, cognitive science, etc. Ideally, all students concentrating on cyber security would be able to take a lab course using a cyber range simulating nodes on a network in a controlled environment. Problem sets could be assigned to groups of students coming from different majors, to give students experience in working with multi-disciplinary teams. Those concentrating in cyber security also should be encouraged to do practical internships.

As noted previously there is no consensus presently on a curriculum for cyber security (see also National Science Foundation Cybersecurity Education Workshop, 2014). This is not necessarily a bad thing, as the field is evolving and it is important for different institutions to be experimenting with different approaches. However, it is also important to be working toward some models that can be widely emulated, which would make it easier for students to switch from one program to another or one institution of higher learning to another, which right now is a challenge due to differing programs and requirements. Students wishing to concentrate on cyber security may fulfill the requirements of a specific major, take required cross-disciplinary foundational courses, a cyber security lab and electives. The cross-disciplinary foundational courses could be a computer science major taking statistics or discrete math courses, a statistics major taking a course on algorithms or programming, etc. More generally, students in computer science, mathematics, statistics, or operations research could be exposed to economics or business courses to gain an understanding of economic costs of cyber attacks and of cyber defense alternatives. Requiring a separate course in economics or business might be "overkill," however, and so once again we return to the idea of developing modules or components in economics or business that would be implemented in courses in computer science, information technology, etc. It might be useful to analyze pre-med curricula as an analogy. Students concentrating on pre-med typically can take a variety of different majors, but require some common foundational courses and lab work. Different majors can lay the groundwork for different cyber security specialties such as cryptography, computer forensics, data security, information assurance, etc.

4.2.5. Key Components of a Successful Cyber Security Education/Training Program

We limit ourselves in this section to a discussion of components of a cyber security education/training program for educating and training the cyber security workforce of the future.

In discussions and interviews, we learned of several components that seem to be central to a successful program

- Because of the multi-disciplinary nature of cyber defense, it is important for students to understand how to work with those in other disciplines
- Learning how to work in teams, where not everyone has every relevant skill.
- Practical experiences through internships or other means.
- Exposure to ways to keep abreast of current research in cyber security.

While some people we talked to felt that it was also necessary to gain exposure to/experience in cyber attacks, not just cyber defense, there was not unanimity on this topic.

It should be noted that cyber security is not just about attacks and defense against attacks. It is much broader than that and includes notions of protection of privacy and proper use of information. There is surely not agreement on what constitutes cyber security, and it may be best to define it in different ways in different contexts or for different target audiences. However, for the purposes of this report, we have adopted the definition given in Section 1.2.

We did hear from many people that cyber security education is not really finished by any means when a student completes a study at a college or university. On-the-job experiences, working with cyber security experts, and lifelong learning are all critical components of building on a college/university degree program in cyber security, and such a program needs to prepare students for the need to gain such continuing exposure and learning.

4.3 Principles of Teaching and Learning Applicable to Cyber Security Education

Questions related to relevant principles of teaching and learning for cyber security education include:

- What are the desired learning outcomes of cyber security education?
- What teaching approaches are most likely to achieve those outcomes?

4.3.1 Desirable Cyber Security Education Outcomes

Long-term retention and transfer are two of the most valued learning outcomes for teaching many different subjects in various settings. Specifically for teaching adults via classes, texts, labs, online components, or informal settings, Halpern and Hakel (2003) summarized the findings of 30 experts from different areas of learning sciences with the claim "The first and only goal: teach for long-term retention and transfer."

While it might seem obvious that long-term retention of concepts and techniques is a desirable goal, many teaching approaches are not designed to accomplish that goal nor do typical tests

measure long-term retention. However, long-term retention is a particularly desirable outcome for cyber security education, because the time at which a student will need to apply what is learned in a classroom or from a textbook can be a long time after the learning takes place. Students answering questions following a typical online tutorial, and those who "cram" for weekly class quizzes or quarterly exams may not have the capability to retrieve information when it is actually needed months later. Specifically in the cyber security context, tools and strategies to aid development of long-term retention skills are needed.

The desirability of knowledge transfer applies to students of all ages and levels. One of the most important functions of the human mind is the ability to use prior knowledge and experience to solve new problems. The learning and cognitive sciences have referred to this as the ability to transfer knowledge or skills from one problem or task to another. This includes transferring prior knowledge and experience to learning new skills and acquiring new knowledge, but also the transfer of this new knowledge and acquisition of new skills to different settings and to solve problems not considered before. Nowhere is this more important than in cyber security education, particularly since we cannot foresee even a small percentage of the problems created by ever changing technology.

There are different types of transfer, near transfer between similarly structured problems and contexts, and far transfer between problems that differ significantly on at least one dimension of knowledge domain, physical context, temporal context etc. (Barnet & Ceci, 2002). Near transfer is the easiest to accomplish and is present in almost all educational environments where a test of knowledge and skills is employed. Far transfer, the most needed for cyber security education, is the hardest to accomplish. Most research and implementation efforts in far transfer have been restricted to math and science and to novice problem solvers. A model introduced by Nokes-Malach and Mestre (Nokes-Malach & Mestre, 2013) consists of a collection of transfer processes including sense making, sacrificing (searching for near optimal solutions that accomplish a set of goals), and a set of mechanisms, which include analogy, identical rules, knowledge compilation, and constraint violation.

The implications for instruction with a successful model of transfer require specifying learner factors such as prior knowledge, experience, and motivation; situational factors such as framing, tasks, tools, and social interaction; and evaluative functions of sense-making and sacrificing (Belenky & Nokes-Malach 2012, 2013), (Richland, Stigler, & Holyoak, 2012). Different types of assessments well suited to the reasoning required in problem solving and the needed behaviors are critical. New approaches to developing skills in far transfer are needed specifically in the cyber security realm.

The modern theory of "learning outcomes" has central importance for cyber security education, and in particular for assessment of effectiveness of such education/training programs and of

cyber security experts. We discuss the notion of "learning outcomes" and its implications for cyber security assessment in Section 4.4.3.

4.3.2 Instructional Approaches that Promote Principles of Teaching and Learning such as Long-Term Retention and Far Transfer

Cyber security education by its very nature requires the learner of all ages to construct their understanding of the cyber world, and become actively involved in the experience of learning. Many researchers have looked at the value of constructivist and experiential learning, some describing them as the same thing, others separating them out as two distinct things. Both theories have the writing and thinking of Jean Piaget as a common ancestor.

We consider constructivist theory of learning to believe that people learn by constructing their own understanding and knowledge of the world, through experiencing things and reflecting on those experiences. When they encounter something new, they have to reconcile it with their previous ideas and experience, maybe changing what they believe, or maybe discarding the new information as irrelevant. Constructivist teachers encourage students to constantly assess how the activity is helping them gain understanding. Particularly in social constructivism approaches, students share their perspectives with other students, enabling a socially constructed understanding beyond what any individual might achieve. This approach is broadly consistent with the importance of cyber security students working in teams. By questioning themselves and their strategies, students in the constructivist classroom ideally become "expert learners."

Experiential learning is learning through reflection on doing, which is often contrasted with rote or didactic learning. In order to gain genuine knowledge from an experience, certain abilities are required:

- The learner must be willing to be actively involved in the experience;
- The learner must be able to reflect on the experience;
- The learner must possess and use analytical skills to conceptualize the experience;
- The learner must possess decision making and problem solving skills in order to use the new ideas gained. (Kolb, 1984)

In either case, the constructivist approach or the experiential approach, the learner constructs a representation of context by framing the task or situation. How knowledge is represented and organized in the mind of the user is critical to framing, construction of a mental representation of "what is going on" based on similar events or experiences from the past. How an individual frames a situation will determine what features of the situation are salient, which in turn impacts what knowledge is activated and applied. Furthermore, the frame that is constructed affects goal setting and the criteria established to evaluate the completion of those goals. Given that different people can frame the same situation differently, it is not surprising that they apply different

knowledge and solution strategies to similar problems. Not only can different people generate different frames, but also the same person can generate different frames depending on the particular features of the situation (Hammer et al., 2005). Different frames may elicit different ways of relating to and participating in new situations – a crucial skill in the rapidly evolving cyber security context. Having framed the task and activated some general knowledge, the learner constructs an initial representation in terms of what is expected and what type of knowledge must be brought to bear. The learner at some point evaluates whether this representation makes sense and moves on to generate a solution to the problem. New tools/techniques are needed to enhance the development of constructivist and experiential learning in the cyber security context. This is a central area for new research that will require partnerships between subject matter experts and educational experts. Some research questions include:

- What backgrounds or prior education/training make a person more likely to benefit from constructivist or experiential learning in the context of cyber security?
- Does the "speed" with which cyber attacks are changing have implications for construction of understanding of the cyber world? Do we understand how a rapidly changing cyber world will make construction of such understanding more difficult or, in some contexts, easier?
- What ways are there to actively involve students in cyber attack and defense in order to be able to conceptualize the experience?
- What are key decision making and problem solving skills needed for experiential learning in the cyber security context?
- How can we best develop social constructivist approaches with the goal of preparing students to work in teams?
- How do individual differences in in framing situations affect/delimit the development of general principles for cyber security learning?

In either case, constructivist or experiential, different types of assessments from testing formats are critical and of their very nature need to be "hands-on". Students frame a high stakes assessment very differently than a low-stakes assessment often in the form of a group project or competition. These different frames affect the level of use and subsequent transfer. It is necessary to develop such assessment tools.

4.4 Cyber Security Education/Training Effectiveness

Questions related to the effectiveness of cyber security education/training include:

- How do we measure the effectiveness of a cyber security education/training program?
- Can we design experiments that will test how best to deliver cyber security training?
- What makes a cyber security expert effective?

4.4.1 Measuring Effectiveness

Ultimately, decisions about what programs in cyber security education/training to invest in depends upon being able to measure the effectiveness of alternative programs. While this is key, we found little agreement on good ways to measure effectiveness and the general impression we have is that there is the need for a great deal of thinking about how to evaluate effectiveness, both of educational/training programs and of the work done by a cyber security expert.

The measurement of effectiveness depends on the desired educational/training objectives, and the cyber security educational/training objectives differ across the student populations we have identified (i.e. the rows of our matrix). We have further subdivided "The Public and K-6" student population into three student groups: The Public, Elementary School, and Middle School. For each student population, there are generally two types of objectives and correspondingly two types of effectiveness measures: those focused on measuring increased awareness of and involvement in cyber security activities, and those focused on actual improvements in cyber security. We should note that the following effectiveness measures are not definitive, but rather suggestions. In each case appropriate effectiveness measure are topics for further research.

The Public:

Objectives: Improved public awareness; improved cyber security for individuals.

Effectiveness Measures for public awareness: Surveys, or perhaps an assessment, of cyber security literacy (the way advertisers measure brand/product awareness); measuring traffic on web sites and social media sites providing cyber security information to the public.

Effectiveness measures for cyber security for individuals: Measuring identity theft, credit card hijacking, botnet attacks, etc. resulting from poor public cyber security practices. However, exactly what is meant by such measures, and what metrics to use, calls for research. So does the question of what other specific types of attacks to develop metrics for.

Elementary School Students:

Objectives: Learning some basic cyber security rules; safer use of the web, games, and smart phones.

Effectiveness Measures for awareness: Age-appropriate cyber security literacy tests.

Effectiveness Measures for safer use of the web, games, smart phones: Results of homework involving parents to establish household rules for using computers and smart phones.

Middle School Students:

Objectives: Increased interest and involvement in learning about cyber security; improved cyber security practices; less cyber bullying.

Effectiveness Measures for awareness: Increased interest in cyber security course modules; increased participation in more advanced computer science and other courses/modules related to cyber security after middle school; increased involvement in school and club cyber security projects, parental involvement in and discussions of home cyber security practices.

Effectiveness Measures for improved cyber security practices: Reduced cyber bullying, use of better passwords, better email practices; monitoring cyber security issues on web sites frequented by middle school children.

Cyber Security Workforce:

Objectives: Expert awareness; more rapid response, i.e. actions to detect, deter, defend, and mitigate cyber security threats to government and commercial networks and systems.

Effectiveness Measures for expert awareness: Attendance at conferences, workshops and tutorials, on-line training courses by professionals focused on cyber security in the workplace – an idea discussed in Section 4.1.1.

Effectiveness Measures for rapid response: Time between earliest detection of a new threat and deployment of means (tools, procedures) to detect, deter, defend and mitigate the new threat. Those responsible for government and commercial networks could keep such data "scorecards" and seek improvement over time. Results of "red team" cyber attacks would be another measure.

High School + College Students in Cyber Security Pipeline:

Objectives: Develop effective and innovative ways to present material and engage students; increase the number of students in the pipeline; and reduce the number of successful cyber attacks targeting high school and college students.

Effectiveness Measures for increasing students in the pipeline: Monitor the number of students preparing for degrees in computer science and related disciplines with particular emphasis on cyber security. Enhance traditional forms of course performance assessment with assessments based on students' building tools and apps that work, and developing web sites to convey cyber security information to other students.

Effectiveness Measures for reducing cyber attacks: Monitor instances of successful phishing attacks and identity thefts on social networking sites.

Other Students Receiving Cyber-Security-Enhanced Education:

Objectives: Increase course enrollment by non-cyber-security pipeline students in courses relevant to cyber security; reduce the number of successful cyber attacks targeting high school and college students.

Effectiveness Measures for course enrollment: New courses or new units in existing course targeting non-specialists (e.g. business students, medical students, liberal arts students, engineering students, etc.). Non-specialist student enrollment in such courses.

Effectiveness Measures for reducing cyber attacks: Monitor instances of successful phishing attacks and identity thefts on social networking sites.

4.4.2 Experiments Testing How to Deliver Cyber Security Training Effectively

There are opportunities to deliver some aspects of cyber security training outside of typical classroom lectures, labs, tutorials, or workshops. Experiments should be designed to explore different modes of training to detect, defend, and mitigate various kinds of cyber attacks such as social engineering and phishing attacks, hoaxes and "urban legends," identity thefts, corrupted software, etc.

There is some evidence (see the "Fish Guru" studies, Kumaraguru et al., 2009) that online cyber security training can be quite effective. However, additional experiments and research should be conducted to test how best to deliver online cyber security training. These experiments need to be carried out both in classrooms and in the workplace. Among the key issues the experiments need to address are:

- When is online training for cyber security superior to other modes of instruction? Do certain types of individuals do better with such training than others? Are certain cyber security topics more amenable to online training than others?
- What are best practices for online cyber security training? These could refer to the frequency of training sessions, the length of those sessions, and the triggers for those sessions.
- How frequently should online training components be modified?
- Does online training work better in large organizations or small ones?
- What are good ways to test the effectiveness of training sessions for cyber security?

Practical implementation of online training may be very difficult. There are likely to be technical, privacy, and ethical issues involved that can be dealt with in a controlled experiment, but are more difficult to resolve in practice.

In addition to online training, there are a variety of types of modes of delivery of cyber security training: virtual reality, games, webinars, tutorials, occasional security briefings, etc.) Questions similar to those involving online training can be raised for each of these areas and experiments for exploring these questions need to be designed.

For all modes of delivery, one set of specific questions to be explored experimentally should focus on the best way to schedule repetitions of training, including the triggers for repetition, the frequency of repetitions (weekly, monthly, quarterly), and the spacing of repetitions. Another set of questions should focus on "teachable moments," i.e. are there specific situations in which the delivery of training would be most beneficial and effective?

Experiments are perhaps best first performed in either a small organization or a small component of a large organization. However, the experiments also should propose means of delivering the training that can scale to a large organization, and can be implemented practically by an organization outside of a controlled experimental environment. On the other hand, another research challenge is whether methods tested in large organizations can be adapted to small organizations.

4.4.3 Assessing the Effectiveness of Cyber Security Experts

It is important to know how various components of cyber security education and training affect the ultimate effectiveness of the cyber security workforce. This question is important for students in the cyber security workforce pipeline and also for the current cyber security workforce as they continue their education/training.

Part of the answer to this question is whether the cyber security expert-in-training acquires the knowledge required for the job. Today, there is not an agreed upon body of knowledge that defines cyber security. Various organizations have defined knowledge requirements for their own operational settings (e.g. see cyber operations/cyber defense requirements from NSA and DHS). The question is, how general are these requirements across all possible cyber security jobs in government, industry, and academia? The National Cyber Security Workforce Framework published by the NIST National Initiative for Cybersecurity Education (NICE) has made a start by standardizing the nomenclature for cyber security jobs. The framework identifies seven categories of cyber security workforce jobs comprising some thirty-one specialty areas and numerous actual position titles. Educators can use this framework as one input to developing curricula for cyber security. However, the NICE framework is a static snapshot of current cyber security jobs. Another input would be the new CAE-IAE criteria. Clearly cyber

security curricula need to lay the groundwork for the future. Until a consensus on education and training requirements emerges, it is impossible to completely assess whether a given program of study will support the effectiveness of cyber security experts.

Besides subject matter knowledge, the presentations and interviews we have collected suggest that additional skills and experience go into making an effective cyber security expert. We have heard, for example, that the cyber security expert must be able to operate effectively as part of a team of people having various backgrounds. This suggests that cyber security training should include team training in which people learn to take on various roles on the team. We have also heard the importance of "soft skills" for cyber security experts. For example, the effective expert must be able to communicate effectively with people who are not steeped in technical knowledge (perhaps the CEO of a company). The reputedly best programs for educating cyber security professionals require internships for practical experience. These internships may provide useful practical settings for acquiring experience in team problem solving and presenting opportunities for "soft skills" development.

Educational principles based on "learning outcomes" and assessments of those outcomes can figure heavily as assessment of cyber security programs and expertise is developed, whether for cyber security experts or even the public at large. "Learning outcomes" are statements of what students are expected to learn in a course or in a class session. The statements are focused on student learning rather than instructor teaching. These statements include a verb phrase and an impact phrase -- what students will be able to do and how they will apply that skill or knowledge. Bloom's taxonomy of educational outcomes (Bloom, 2003) includes the following as "cognitive skills":

Knowledge/remembering
Comprehension/understanding
Application/applying
Analysis/analyzing
Evaluation/evaluating
Synthesis/creating

In the case of cyber security, we should develop goals for each of these cognitive skills. The following are all measurable, according to educational theory:

- Knowledge: define, list, recognize
- Understanding: characterize, describe, explain, identify, locate, recognize, sort
- Application: choose, demonstrate, implement, perform
- Analysis: analyze, categorize, compare, differentiate
- Evaluation: assess, critique, evaluate, rank, rate

- Synthesis: construct, design, formulate, organize, synthesize

For example, we might ask that a student or cyber security expert be able to:

- Understand and be able to identify the source of an anomaly
- Discuss, interpret, and ascribe meaning to the data shown in a network status report
- Be able to evaluate the impact of a change in access control
- Be able to analyze a denial of service attack and develop a response to reflect this analysis.
- Discriminate among different types of cyber attacks
- Analyze current research findings in the area of security of cross-site forgeries

"Learning progressions" are descriptions of the successively more sophisticated ways of thinking about a topic as one learns about and investigates a topic over a span of time. This concept began to be used in 2005 and has a likely usefulness in describing appropriate progressions for different levels of cyber security expertise or awareness.

Assessment is based on what we value, so learning outcomes determine assessment. Assessment calls for planning ahead, designing and implementing data collection approaches, and revising assessments as we progress. Good assessment provides direct evidence of learning and uses a variety of assessment tools. Some techniques of assessment in educational theory are based on "immediate feedback." These include:

- Minute papers – teachers ask students at the end of the class, or week, to write a few sentences about what they learned during the class(es), and their most important unanswered question(s).
- Critical incident reports – capture vivid happenings that the student considers significant (compare "teachable moments" discussion above).
- Journals – document the learning taking place throughout the course, reviewed after each exam or test.
- Reflections – similar to minute papers

Longer-term assessments include:

- Exams
- Performance assessments – performances, projects, oral presentations, simulations, etc.
- Portfolios
- Juried activities – multiple raters
- Standardized test banks

It would be good to use each of these categories to design assessments for different levels of cyber security expertise and awareness. For instance, can we develop specific ideas for the use of journals in cyber security education courses or modules? Can we design a concept of portfolio for a cyber security expert and ways to assess such a portfolio? Can we develop standardized test banks for cyber security expertise at different levels?

5. Some Recommendations

We start this section with some general principles based on our research. A general recommendation is that DHS take these general principles into account in deciding on its investments in cyber security education and training. We then divide our recommendations into three subsequent sections, one dealing with Education and Training, a second with the Workforce (including Workforce Development), and the third dealing with needed research. In each section of those three sections we highlight a few ***key recommendations*** and then list others.

5.1. General Principles for Cyber Security Education and Training

5.1.1. Fundamentals of Education and Training

a. A key component of any Cyber Security Education and Training Program, whether for specialists or generalists, should be the identification of principles of cyber behavior that endure under changing threats, responses, or devices.

b. The body of cyber security knowledge cannot be static but must allow for dynamic adaptation and extension. This will allow users of iPads and smartphones, as well as users of social media such as FaceBook and Twitter, to have personalized learning/training related to their devices and the way they use them. As new research allows Recommender Systems to become more and more sophisticated, we can expect such personalized learning/training to be expanded to all kinds of contexts, whether for unsophisticated or sophisticated users.

c. An education or training program should be built on principles of teaching and learning, for example principles of transfer and repetition, and these principles in turn should be used in determining effectiveness of different approaches.

d. Cyber security education and training initiatives have grown in a mostly uncoordinated fashion. There is need to give them a firm grounding in education principles and to base them in a broader collection of relevant disciplines than just computer science, information technology, and computer engineering. Specifically, there is need to ground programs in social and management science and cognitive science.

e. The problems of cyber security are fundamentally multidisciplinary. This implies the need for education and training in how to work with people in other disciplines, and in particular how to work in multidisciplinary teams.

f. Just as cyber security education/training should emphasize multidisciplinarity, we can learn from other fields how they are developing programs for introducing mulidisciplinarity. We can also learn from educational innovations in such fields as education in medicine, public health, business, engineering, and the military.

g. Research and education/training should be intimately connected, in two ways: (1) current research in cyber security should find its way into education/training programs as rapidly as possible; (2) new education/training programs should be developed in connection with research into what programs are most effective.

h. It is important to develop ways to measure effectiveness of (1) cyber security education programs; (2) cyber security experts. These criteria should be used when making decisions about investment in cyber security education and training.

i. Sharing information, experiences, and best practices is an important way to keep employees, partners, and educational programs current.

5.1.2. Target Audience

a. The target audience for cyber security education/training includes the current and future workforce in DHS, in the HSE, and in the public and private sector. It also includes students at all levels from pre-K through graduate school. And it includes the public at large. New programs should be age-appropriate and background-appropriate and research should underlie determination of what is appropriate.

b. Input in developing programs should come from a variety of sectors, agencies, organizations, and the public at large, and should include an international component since cyber security is an international problem.

c. The appropriate age at which to start cyber security awareness and education needs to be determined through research, but it is likely to be very young.

5.1.3. Timing of Changes

a. Development of cyber security education and training programs needs to proceed with differing goals for the near-term, medium-term, and long-term. For us, near-term means a matter of months, medium-term means less than a year, and long-term means a few years. However, there must also be an "ultra long-term" point of view – which addresses the need for general workforce awareness, general public awareness, and development of specialists. What is done in the near-, medium-, and long-term in programs must connect to this ultra long-term view.

5.2. Specific Recommendations for Education and Training

Key Recommendation 5.2.1: ***Teams***. Put an emphasis on education and training to work in teams. Learn from education in other fields (medicine, public health, engineering, business, etc.) how cyber security experts might be trained to work in teams and how they might be educated to use their knowledge and experience to address situations they have not seen before.

Key Recommendation 5.2.2: ***Internships***: Internships are a key way to enhance contextual, on-the-job learning, which is a key component of cyber security education and training and is centrally related to day to day operations in the cyber security role. DHS should encourage the Homeland Security Enterprise (HSE) to develop internship opportunities for college/university students interested in cyber security, and work with the private sector to develop cyber security internship opportunities for HSE employees in the private sector. Also develop internship opportunities in leading cyber security programs in the private sector or other government agencies for DHS cyber security experts. Internships are critical and require a serious commitment by the sponsor. Too often, they are sacrificed when budgets are cut. As part of any internship program, it is also important to raise the question of "what next" after an internship.

Key Recommendation 5.2.3: ***Teacher Development***: DHS should invest in programs that will assist teachers at universities, 4-year, and 2-year colleges, and some high schools to become proficient at teaching cyber security courses, and providing team exercises and hands-on experiences. A variety of approaches should be tried, including coursework, tutorials, summer workshops, the establishment of cyber security centers, and internships. The internships should be bi-directional, i.e. teachers being placed in government and industry cyber security groups, and cyber security experts from government and industry being placed with academic departments.

Key Recommendation 5.2.4: ***Module Development and Certification***. Because the curriculum (whether K-12, undergraduate, graduate) is crowded and has many interests in play, shorter components may be easier to initiate than longer ones. DHS should encourage development of more modules on cyber security topics that can be used in different courses of study (e.g. computer science, statistics, mathematics, engineering, business but also sociology and economics and cognitive science) for short periods of time ranging from a day to a week, including some for courses not intended for cyber security specialists or even majors in areas such as computer science, computer engineering, or information technology, and including courses at the precollege level. (Note that there are many modules being developed for specialists and for practical training, but the modules we have in mind include those for the general student.) Evaluate natural sequences in different college/university majors into which modules can be introduced. With any new materials, testing and certification is critical. Such testing is best done by a formal evaluator with educational evaluation experience who interviews

both teachers and students before and at several stages after the module is used. It is important to identify in advance those hypotheses the evaluator is testing or desirable outcomes that the module is designed to achieve.

Key Recommendation 5.2.5: ***Engage More Disciplines***: Put increasing emphasis on additional important topics for cyber security education: learning science, psychology, sociology economics, political science. (Note for example that the Air Force Academy has a political science course as the second key course in cyber security education offered to cadets.)

Recommendation 5.2.6: ***Educating The Public***: Assess what is available to educate the public about cyber security. Evaluate how many people of different demographics receive this education. Evaluate the effectiveness of the various methods of delivery employed and the completeness of the coverage.

Recommendation 5.2.7: ***Age-appropriate Cyber Security Literacy Metrics***. Develop age-appropriate cyber security literacy metrics and use these to evaluate the effectiveness of various programs. Support the development of online training, including games and apps that encourage people to assess their individual literacy and try to improve it.

Recommendation 5.2.8: ***Pathways to Cyber Security Specialization***. Consider the pathways that students might use to move from generalists to technical majors (e.g. computer science, mathematics, statistics, computer engineering) to majors in a cyber security specialist-related field. Find ways to minimize the delay in moving from the generalist category to the technical major category and from the technical major category to the cyber security specialist category should a student develop an interest in doing so.

Recommendation 5.2.9: ***Learning Progressions***. Develop "learning progressions" (see Section 4.4.3) for the development of different levels of cyber security expertise and awareness.

Recommendation 5.2.10: ***Assessment Procedures***. Develop assessment tools in general and for constructivist and experiential learning specifically, distinguishing between high-stakes and low-stakes assessment. Develop specific assessment procedures corresponding to "immediate feedback" and longer-term assessments, such as the "journals" and "portfolios" discussed in Section 4.4.3.

Recommendation 5.2.11: ***Cyber Security Lab Projects***. Develop more cyber security lab projects that can be run in cyber range virtual environments by university students and cyber security workforce employees. Some of the projects should require teams of students (possibly from different disciplines) working together.

5.3. Specific Recommendations for Existing Workforce and Workforce Development

Key Recommendation 5.3.1: ***Sharing***. Sharing information and "best practices" is a good way to keep up with evolving challenges. This is especially relevant to "on the job learning" and "adaptive learning" that addresses how today's subject matter expert in one discipline needs to be a life-long learner to keep up with new disciplines and rapidly changing contexts in which to apply the discipline in which they were trained. DHS could play a major role here in enhancing already-existing approaches to information sharing by developing updates and best practices guides both for new approaches to cyberdefense and to education/training, to be shared across its components and also with the Homeland Security Enterprise and the private sector. Enhanced methods to share in the reverse direction would also be very useful. Making use of professional societies (as is done in Engineering education) and state and local homeland security agencies can help a great deal in information sharing initiatives.

Key Recommendation 5.3.2: ***Improve Interaction with ISACs***. DHS already interacts with numerous ISACs, but services differ and sharing can be improved. DHS should study NCCIC interactions with the ISACs, and establish a set of best practices that can be deployed with every ISAC. DHS should also analyze whether new information sharing technologies can be deployed to improve interactions with ISACs, and explore other methods for making the ISACs an even better conduit for alerting, educating, and training the HSE in cyber security.

Key Recommendation 5.3.3: ***Cognitive Skills Goals***. Develop specific examples of cognitive skill goals for cyber security experts in terms of knowledge/remembering, comprehension/understanding, application/applying, analysis/analyzing, evaluation/evaluating, and synthesis/creating.

Key Recommendation 5.3.4: ***Small Organizations***. Consider the special needs in terms of cyber security education/training for small businesses or smaller agencies in the Homeland Security Enterprise, where dedicated cyber security expertise and extensive continuing education may not be feasible.

Recommendation 5.3.5: ***Certification***. Explore the possibility of levels of certification for specialized cyber security experts analogous to "Board Certification" for medical experts or levels of certification for engineers. The intent here is not to set up barriers for people beginning careers in cyber security, which for the time being would not have certification, but rather to ensure that more advanced cyber security workforce experts continue to keep pace with evolving technical issues.

Recommendation 5.3.6: ***Performance Metrics for IT Organizations***. Develop and standardize cyber security performance metrics for IT organizations, and distribute them to IT departments at

government agencies and private businesses. Develop ways to survey the IT departments periodically and ask them to report their current performance (perhaps anonymously). Publish aggregate results for different groups of businesses and agencies.

Recommendation 5.3.7: ***Recruit Women***. Develop programs to encourage more women to go into cyber security, in order to increase both the size and the diversity of the cyber security work force.

Recommendation 5.3.8: ***Online Knowledgebase of Cyber Threats***. Develop an extensible (e.g. "crowd sourceable") online knowledgebase of information sources regarding cyber threats. Develop a query and retrieval architecture enabling people to use the knowledgebase to classify and understand various new types of cyber threats as they encounter them (see CCICADA work on Smart Notes tool and Personal Security Assistant described in Section 4.1.3).

5.4. Specific Recommendations for Research

Key Recommendation 5.4.1: ***Defining the Cyber Security Body of Knowledge.*** Encourage research to establish a definitive body of knowledge for the discipline of cyber security. This work is crucial for curriculum development, and possible future accreditation, certification and professionalization efforts. The research should draw on existing efforts such as ACM ITiCSE 2011, the ACM 2013 working group, the ACM/IEEE CS2013, the CAE-IAE criteria, and the National Science Foundation Cybersecurity Education Workshop recommendations. The body of cyber security knowledge cannot be static, but must allow for dynamic adaptation and extension.

Key Recommendation 5.4.2: ***Better Metrics for Effectiveness.*** Encourage research to identify metrics for effectiveness of cyber security education and training for each of the student groups described. For each group, metrics need to be developed for improving cyber security awareness, as well as improving cyber security practices.

Key Recommendation 5.4.3: ***When and How to Begin Cyber Security Education***. Encourage research to determine the appropriate age to begin cyber security education and to determine the "sweet spot" at which to start serious exposure to cyber security; in particular determine whether middle school is that sweet spot.

Key Recommendation 5.4.4: ***Transfer and Repetition***. Encourage research on alternative modes of teaching to emphasize concepts of transfer and repetition into cyber security education and training for the DHS workforce, and design experiments to test the effectiveness of different modes of delivery and the frequency and spacing of repetitions. Do the same for college/university settings, middle school, high school, and elementary school.

Recommendation 5.4.5: ***Modes of Delivery***. Develop experiments to determine how effective modes of delivery may differ depending upon the type of organization (school, university, business or agency) the size of the organization whose employees are being educated, the age of the learners, and how they may differ for different learning outcomes used to drive the education.

Recommendation 5.4.6. ***Far Transfer***. Develop and test specific strategies that enable students to accomplish far transfer between cyber security problems that differ significantly on at least one dimension of knowledge domain, physical context, temporal context etc.

Recommendation 5.4.7. ***Constructivist and Experiential Learning***. Develop and test tools/techniques to aid students and lifelong learners attain the skills for constructivist and experiential learning in the cyber security context.

Recommendation 5.4.8. ***Long-term Retention***. Develop and test specific strategies to aid long-term retention and application of cyber security knowledge and principles.

6. References

[1] ACM/IEEE-CS Joint Task Force on Computing Curricula. 2013. Computer Science Curricula 2013. ACM Press and IEEE Computer Society Press. http://www.acm.org/education/CS2013-final-report.pdf

[2] Albrechtsen, Eirik, and Jan Hovden. "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study." *Computers & Security* 29, no. 4 (2010): 432-445.

[3] Avery, Jeff. "A Study of Phishing Defense methods." Ph.D. dissertation, Purdue University, 2013.

[4] Baker, M. "State of Cyber Workforce Development." White paper, Software Engineering Institute, CERT Division, August, 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=83504

[5] Barnett, S. M., and S. J. Ceci. "When and where do we apply what we learn? A taxonomy for far transfer." *Psychological Bulletin* 128 (2002): 612–637.

[6] Beers, R. Written testimony of DHS Acting Secretary Rand Beers for a Senate Committee on Homeland Security and Governmental Affairs hearing titled "Threats to the Homeland" Release Date: November 14, 2013

[7] Belenky, D.M., and T. J. Nokes-Malach. "Mastery-approach goals and knowledge transfer: An investigation into the effects of task structure and framing instructions." *Learning and Individual Differences* 25 (2013): 21–34.

[8] Bloom, B. S., M. D. Engelhart, E. J. Furst, W. H. Hill, and D. R Krathwohl. *Taxonomy of educational objectives: the classification of educational goals; Handbook I: Cognitive Domain.* New York: Longmans, 1956.

[9] Chapman, Ian M., Sylvain P. Leblanc, and Andrew Partington. "Taxonomy of cyber attacks and simulation of their effects." *Proceedings Military Modeling & Simulation Symposium MMS.* 2011.

[10] College Board: New Course and Exam – AP Computer Science: Principles to Launch in Academic Year 2016-2017. http://www.collegeboard.com/html/computerscience/

[11] College Board Press Release: The National Science Foundation Provides $5.2 Million Grant to Create New Advanced Placement® Computer Science Course and Exam, June 13, 2013. http://press.collegeboard.org/releases/2013/national-science-foundation-provides-52-million-grant-create-new-advanced-placement-compute

[12] Cone, Benjamin D., Cynthia E. Irvine, Michael F. Thompson, and Thu D. Nguyen. "A video game for cyber security training and awareness." *Computers & Security* 26, no. 1 (2007): 63-72.

[13] Conklin, A. "Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course." *System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on.* 2006. 220b-220b.

[14] Dodge, Ronald C., Jr., Curtis Carver, and Aaron J. Ferguson. "Phishing for user security awareness." *Computers \& Security* 26, no. 1 (2007): 73-80.

[15] Exploring Computer Science: http://www.exploringcs.org/resources/cs-statistics

[16] Freedberg, Jr., S.J. "National Guard Fights for Cyber Role in 2015 Budget." Breaking Defense, February 5, 2014. http://breakingdefense.com/2014/02/national-guard-fights-for-cyber-role-in-2015-budget/

[17] GAO-13-187. Cybersecurity. National Strategy, Roles, and Responsibilities Need to be Better Defined and More Effectively Implemented. United States Government Accountability Office, February, 2013.

[18] Halpern, Diane F, and Milton D Hakel. "Applying the science of learning to the university and beyond: Teaching for long-term retention and transfer." *Change: The Magazine of Higher Learning* (Taylor \& Francis) 35, no. 4 (2003): 36-41.

[19] Hammer, D., A. Elby, R. E. Scherr, and E. F. Redish. "Resources, framing, and transfer." Edited by J. Mestre. *Transfer of learning from a modern multidisciplinary perspective.* Greenwich, CT: Information Age, 2005. 89–-119.

[20] Harley, David, and Andrew Lee. "Phish Phodder: Is User Education Helping or Hindering." *Virus Bulletin Conference.* 2007. http://www.smallblue-greenworld.co.uk/davidharleyandrewleevb2007.pdf

[21] Hsu, D.Frank, and Dorothy Marinucci. *Advances in Cyber Security.* Edited by D.Frank Hsu and Dorothy Marinucci. Fordham University Press, 2013.

[22] “ISC2 Internet security education foundation.” *ISC2 Internet security education foundation.* Kolb, David A, and others. *Experiential learning: Experience as the source of learning and development.* Vol. 1. Prentice-Hall Englewood Cliffs, NJ, 1984. https://www.isc2cares.org/safe-and-secure/

[23] Kahan, J.H. “What’s in a name? The meaning of Homeland Security.” *Journal of Homeland Security Education*, vol 2 (2013), 1-18.

[24] Kritzinger, E., and S.H. von Solms. "Cyber security for home users: A new way of protection through awareness enforcement." *Computers & Security* 29, no. 8 (2010): 840-847.

[25] Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M.A., Pham, T. "School of phish: a real-world evaluation of anti-phishing training." *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09)*. New York, NY, USA, 2009. http://dl.acm.org/citation.cfm?doid=1572532.1572536

[26] Loukas, George, Diane Gan, and Tuan Vuong. "A taxonomy of cyber attack and defence mechanisms for emergency management networks." *Proceedings of PERCOM.* 2013.

[27] Lute, J., Durrance, D., and Uenuma, M. “Mission Critical CyberSecurity Functions.” Council on CyberSecurity, February, 2014. http://www.counciloncybersecurity.org/attachments/article/51/Mission%20Critical%20CyberSecurity%20Functions_Narrative.pdf

[28] Mestre, J. P., B. H. Ross, D. T. Brookes, A. D. Smith, and T. J Nokes. "How cognitive science can promote conceptual understanding in physics classrooms." In *Fostering scientific habits of mind: Pedagogical knowledge and best practices in science education*, edited by I. M. Saleh and M. S.Khine, 3–8. Rotterdam, The Netherlands: Sense, 2009.

[29] Mundie, David, and David McIntire. "The MAL: A Malware Analysis Lexicon." Tech. rep., Software Engineering Institute CMU, 2013.

[30] National Cyber Security Alliance In Brief. http://www.whitehouse.gov/files/documents/cyber/National%20Cyber%20Security%20Alliance%20in%20Brief%203%209%2009.pdf

[31] "National Cybersecurity Workforce Framework." *National Cybersecurity Workforce Framework.* NIST, 2013. http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing.pdf

[32] National Science Foundation (2014).Cybersecurity Education Workshop, February 24-25, 2014, George Washington University Arlington Center, Arlington, VA. Final Report, April 7, 2014.
https://research.gwu.edu/sites/research.gwu.edu/files/downloads/CEW_FinalReport_040714.pdf

[33] Niekerk, J.F. Van, and R. Von Solms. "Information security culture: A management perspective ." *Computers \& Security* 29, no. 4 (2010): 476-486.

[34] Nokes,-Malach, T.J., and Mestre, J.P. "Toward a model of transfer as sense-making." *Educational Psychologist* 48 (3) (2013), 184-207.

[35] *NSA CryptoKids Online Games.* http://www.nsa.gov/kids/home.shtml.

[36] Richland, L. E., J. W. Stigler, and K. J Holyoak. "Teaching the conceptual structure of mathematics." *Educational Psychologist* 47 (2012): 189–203.

[37] Schaffhauser, Dian. *Teens' Online Safety Improved by Education, Research Shows.* 2008. http://thejournal.com/articles/2008/11/25/teens-online-safety-improved-by-education-research-shows.aspx.

[38] School CIO (2013). "AP Computer Science MOOC Enrolls Nearly 1300." School CIO, September 16, 2013. http://www.schoolcio.com/cio-back-office-business/0104/ap-computer-science-mooc-enrolls-nearly-1300/54233

[39] Security Injections @ Towson: http://cis1.towson.edu/~cssecinj/

[40] Shaw, R.S., Charlie C. Chen, Albert L. Harris, and Hui-Jou Huang. "The impact of information richness on information security awareness training effectiveness." *Computers \& Education* 52, no. 1 (2009): 92-100.

[41] Sheng, S., et al. "Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish." *SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security.* 2007. 88–99.

[42] "Small Business Cyber Security Guide." University of Southern Maine, 2013. https://www.maine.gov/ag/docs/Small-Business-Cyber-Security-Guide.pdf

[43] Spidalieri, Francesca, "Joint Professional Military Education Institutions in an Age of Cyber Threat. Pell Center for International Relations and Public Policy, Salve Regina University, 2013. http://pellcenter.salvereginablogs.com/files/2013/08/JPME-Cyber-Leaders-Final.pdf

[44] Spidalieri, Francesca, "One Leader at a Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat." Pell Center for International Relations and Public Policy, Salve Regina University, 2013. http://pellcenter.salvereginablogs.com/files/2013/04/One-Leader-at-a-Time-FINAL.pdf

[45] Stewart, Kyle E., Jeffrey W. Humphries, and Todd R. Andel. "Developing a virtualization platform for courses in networking, systems administration and cyber security education." *Proceedings of the 2009 Spring Simulation Multiconference*. San Diego, CA, USA: Society for Computer Simulation International, 2009. 65:1--65:7.

[46] Thomas, Kim. "Teen online & Wireless Safety Survey." 2009. http://ww2.cox.com/wcm/en/aboutus/datasheet/takecharge/2009-teen-survey.pdf?campcode=takecharge-research-link_2009-teen-survey_0511.

[47] U.S. Department of Homeland Security (2012). Homeland Security Advisory Council, Cyber Skills Taskforce Report. Fall, 2012. http://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf

[48] Verizon's 2012 Data Breach Investigations Report. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf

[49] Zweben, S. Computing Degree and Enrollment Trends: From the 2011-2012 CRA Taulbee Survey. Computing Research Association, 2013. http://cra.org/govaffairs/blog/wp-content/uploads/2013/03/CRA_Taulbee_CS_Degrees_and_Enrollment_2011-12.pdf

7. Project Team

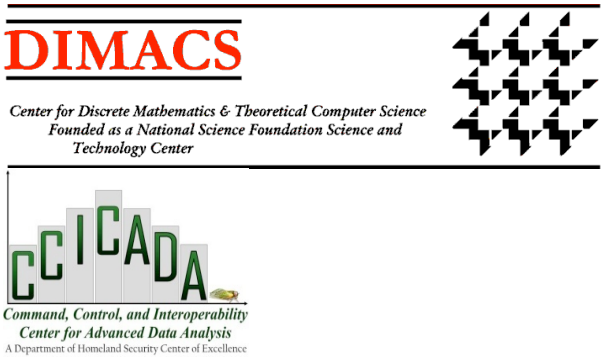
Rutgers, the State University of New Jersey
Professor Fred S. Roberts
Professor Rebecca Wright
Professor Dennis Egan
Professor Margaret "Midge" Cozzens
Professor Paul Kantor
Professor Eugene Fiorini
Dr. Brian Ricks, Post-Doctoral Associate
Jason Perry, Graduate Student
Curtis McGinity, Graduate Student

Stevens Institute of Technology
Professor Susanne Wetzel
Luke Scholl, Graduate Student

Carnegie Mellon University
Professor Eduard Hovy
David Klaper, Graduate Student
Navneet Rao, Graduate Student

8. Appendices

8.1 Brainstorming Workshop Participants



WORKSHOP: ***Cyber Security Education Brainstorming***
October 7, 2013: 10am to 4pm

WORKSHOP ATTENDEES (v) = virtual

James Abello
Rutgers University

Owen Astrachan
Duke University

Kaethe Beck
Purdue University & VACCINE (v)

Terry Benzel
University of Southern California/Information Sciences Institute (v)

Lora Billings
Montclair State University (v)

Dan Boneh
Stanford University (v)

Scott Buck
INTEL (v)

Diana Burley
George Washington University (v)

Steve Cooper
Stanford University (v)

Midge Cozzens
Rutgers University

Melissa Dark
Purdue University (v)

Nicole Dean
Raytheon

Giovanni DiCrescenzo
Applied Communications Sciences

Ronald Dodge
US Military Academy (v)

Dennis Egan
Rutgers University

Mitch Errickson
US Department of Homeland Security

Dave Evans
University of Virginia (v)

Michalis Faloutsos
University of New Mexico (v)

Nina Fefferman
Rutgers University

Eugene Fiorini
Rutgers University

Peter Freeman
Georgia Tech. (CCICADA Advisory Bd.) (v)

Michael Gochfeld
Rutgers Medical School

Gerald Goldin
Rutgers University

William Hery
NYU-Polytechnic Institute

Mark House
Associated Press

Eduard Hovy
Carnegie Mellon University (v)

Frank Hsu
Fordham University

Aaron Jaggard
Colgate University (v)

Rebecca Jordan
Rutgers University

Paul Kantor
Rutgers University

Joseph Kielman
US Department of Homeland Security (v)

Robert Laumbach
Rutgers University

Curtis McGinity
Rutgers University (v)

Nasir Memon
NYU-Polytechnic Institute (v)

Jelena Mirkovic
University of Southern California/Information Sciences Institute (v)

Brian Nakamura
Rutgers University

Christie Nelson
Rutgers University

Robert M. Panoff
Shodor Education Foundation (v)

Jason Perry
Rutgers University

Davina Pruitt-Mentle
Educational Technology Policy, Research and Outreach; National CyberWatch Center & University of Maryland

Raj Rajagopalan
Honeywell (v)

Golden G. Richard III
University of New Orleans (v)

Brian Ricks
Rutgers University

Fred Roberts
CCICADA Director
Rutgers University

Dan Roth
University of Illinois at Urbana-Champaign (v)

Emily Saulsgiver
US Department of Homeland Security (v)

Luke Scholl
Stevens Institute of Technology

Katie Shilton
University of Maryland (v)

Deborah Silver
Rutgers University

John Stasko
Georgia Tech. & VACCINE (v)

Scott Stornetta
Columbia High School – Maplewood NJ

Patricia Tamburelli
County College of Morris

Costis Toregas
George Washington University

Scott Tousley
US Department of Homeland Security

Michael T. Vance
NJ Office of Homeland Security and Preparedness

Susanne Wetzel
Stevens Institute of Technology

Trefor Williams
Rutgers University

James Wojtowicz
Rutgers University

Rebecca Wright
DIMACS Director
Rutgers University

8.2 Panels for Brainstorming Workshop

Panel No. 1: Government/University
Facilitator: Rebecca Wright, Director of DIMACS, Rutgers University
Theme: What is happening now at government agencies and universities and what might be needed.
Susanne Wetzel, Stevens Institute of Technology
Michael Vance, NJ Office of Homeland Security and Preparedness
Ronald C. Dodge, Jr. United States Military Academy (virtual)
Patricia Tamburelli, County College of Morris
Melissa Dark, Purdue University (virtual)

Panel No. 2: Private Sector
Facilitator: Dennis Egan, CCICADA Research Faculty, Rutgers University
Theme: What is happening now in the private sector and what might be needed.
Raj Rajagopalan, Honeywell (virtual)
Mark House, Associated Press
Nicole Dean, Raytheon
Scott Buck, INTEL (virtual)

Panel No. 3: Education Principles of Teaching and Learning for Cyber Security Education
Facilitator: Fred S. Roberts, Director of CCICADA, Rutgers University
Theme: What general principles of teaching and learning, based on educational theory, will aid us in evaluating and choosing new cyber security educational programs.
Midge Cozzens, Rutgers University
Owen Astrachan, Duke University
Robert M. Panoff, Shodor Education Foundation (virtual)
Eugene Fiorini, Rutgers University

Panel No. 4: Learning from Analogies

Facilitator: Fred S. Roberts, Director of CCICADA, Rutgers University

Theme: What can we learn from medical school education, public health education for the public, energy-efficient behavior education, education of the military, etc.

Michael Gochfeld, Rutgers-Robert Wood Johnson Medical School – Environmental and Occupational Health Sciences Institute

Lora Billings, Montclair State University (virtual)

Nina Fefferman, Rutgers University

Dennis Egan, Rutgers University

Deborah Silver, Rutgers Universtiy

Panel No. 5: K-12 and Informal Public Cyber Security Education

Facilitator: Midge Cozzens, CCICADA Director of Education, Rutgers University

Theme: What is happening in K-12 and public education, including adult education and public informal education.

Davina Pruitt-Mentle, Educational Technology Policy, Research and Outreach; National CyberWatch Center & University of Maryland

Katie Shilton, University of Maryland (virtual)

Scott Stornetta, Columbia High School, Maplewood, NJ

Nasir Memon, Polytechnic Institute of NY (virtual)

Rebecca Jordan, Rutgers University

Panel No. 6: Tools of Delivery for Effective Cyber Security Education

Facilitator: Susanne Wetzel, Stevens Institute of Technology

Theme: Discuss modes of presentation (online, videos, use of apps), frequency (monthly updates, retraining,), use of technology (games, virtual reality), and tie these in to teaching and learning.

Kaethe Beck, Purdue University (virtual)

Costis Toregas, George Washington University

Curtis McGinity, Rutgers University (virtual)

8.3 Subject Matter Experts Contacted for Further Information by Phone or Email

Lora Billings, Professor of Applied Mathematics, Department of Mathematical Sciences, Montclair State University

Martin C. Carlisle, Professor, Department of Computer Science, US Air Force Academy, and Direcor, Academy Center for Cyberspace Research

David Evans, Professor of Computer Science, University of Virginia

Mark Hagerott, Deputy Director and Distinguished Professor, Center For Cyber Studies, US Naval Academy

Mark House, Information Security, The Associated Press

D. Frank Hsu, Professor of Computer Science & Information Science, Department of Computer & Information Sciences, Fordham University

Katherine Worboys Izsak, Associate Director for Education, National Consortium for the Study of Terrorism and Responses to Terrorism (START)

Rebecca Jordan, Associate Professor of Environmental Education and Citizen Science, School of Environmental and Biological Sciences, Rutgers University

Jane Holl Lute, President and Chief Executive Officer, Council on CyberSecurity, and former Deputy Secretary of Homeland Security

Douglas Maughan, Director, Cyber Security Division, DHS Science & Technology Directorate

Ernest McDuffie, Lead for National Initiative for Cybersecurity Education (NICE), National Institute of Standards and Technology

Vice Admiral Charles D. Michel, Deputy Commandant for Operations, United States Coast Guard

Paul A. Pietropaulo, Corporate Information Security Officer, Office of the Secretary, The Port Authority of New York and New Jersey

Victor Piotrowski, Lead Program Director, National Science Foundation

Steve Richards, Associate Directory of Communications and Training, DHS Privacy Office

John Riley, Branch Chief, Digital Forensics Branch, Federal Law Enforcement Training Center, Department of Homeland Security

Eugene Spafford, Professor of Computer Science, Purdue University

Francesca Spidalieri, Fellow for Cyberleadership, Pell Center for International Relations and Public Policy, Salve Regina University

W. Scott Stornetta, Teacher of Mathematics, Columbia Senior High School, Maplewood, NJ

8.4 Matrix of Resources

Cyber Security Education Category/Topic Matrix:

Population	**Existing programs and centers targeted at these learners**	**Educational principles that apply to these learners**	**Analogous other kinds of educational efforts**	**Modes of delivering the educational content**	**Journals, Standards and Reports on the state of the art for educating this population**
Category 1: Public awareness and K-6 education	US-CERT http://www.us-cert.gov/ NJ InfoSecure http://www.nj.gov/njinfosecure/ Canada centre for digital and media literacy http://mediasmarts.ca/cyber-security/ [22] "ISC2 Internet security education foundation." https://www.isc2cares.org/safe-and-secure/	Awareness Albrechtsen , Hovden [2], Kritzinger, von Solms [24] Attention, memorableness, generating excitement Targeting specific age groups	Public health Rutgers http://sph.umdnj.edu/	Brochures, flyers PSA's Billboards Twitter feeds Online games [35] *NSA CryptoKids Online Games.* http://www.nsa.gov/kids/home.shtml. [12] , [41]	iKeepSafe c3 matrices http://www.ikeepsafe.org/educators/more/c3-matrix/ NICE: "Cybersecurity in K-12" http://csrc.nist.gov/nice/Sept2011-workshop/presentations/Thursday/Thurs_Cuny_NICE_K-12_092211.pdf [46] Thomas, Kim. "Teen online & Wireless Safety Survey." 2009. http://ww2.cox.com/wcm/en/aboutus/datasheet/takecharge/2009-teen-survey.pdf . Phishing [14] "Phishing for user security awareness." http://repository.cmu.edu/cgi/viewcontent.cgi?article=1011&context=cylab [20] "Phish Phodder: Is User Education Helping or Hindering." http://www.smallblue-greenworld.co.uk/davidharleyandrewleevb2007.pdf

Category 2: Workforce with cyber security responsibilities	International Conference on Cyber Security (ICCS) http://iccs.fordham.edu/ DHS Employee training National Guard [16] Raytheon cyber-operator course http://www.raytheon.com/ourcompany/rtnwcm/groups/rtsc/documents/content/rtn_b_rtsc_cyber_brochure.pdf U. Miami "Computer Security at work" http://it.med.miami.edu/x907.xml [43] Spidalieri, Francesca, "Joint Professional Military Education Institutions in an Age of Cyber Threat. http://pellcenter.salvereginablogs.com/files/2013/08/JPME-Cyber-Leaders-Final.pdf	Institutional Culture [33] Niekerk, J.F. Van, and R. Von Solms. "Information security culture: A management perspective." Building operational knowledge Teaching social/anthropological as well as technical principles Problem-based, collaborative, inquiry-based, experiential Teacher/ adult learner equality Determining needed frequency	Occupational Safety Training Security first responders	Workplace training modules Email lists Employee Security Guide Documents: [42] "Small Business Cyber Security Guide." U of Southern Maine, 2013. https://www.maine.gov/ag/docs/Small-Business-Cyber-Security-Guide.pdf Embedded OTJ awareness training [25] Kumaraguru, Cranshaw, Acquisti, Cranor, Hong, Blair, Pham. "School of phish: a real-world evaluation of anti-phishing training." http://dl.acm.org/citation.cfm?doid=1572532.1572536 Larger-scale Exercises	Information Systems and Security Education Journal Functions and advances: Hsu, Marinucci [21], Lute, Durrance, and Uenuma [27], Baker [4] [48] Verizon's 2012 Data Breach Investigations Report. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf [31] "National Cybersecurity Workforce Framework." NIST, 2013. http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing.pdf Phishing Defense Survey NIST CSRC SP 800-50: Building an IT Security Awareness and Training Program http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf NIST CSRC 800-16: IT Security Training Requirements: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf

Category 3: High School and College Students in Cyber Security Pipeline	DHS NICCS http://niccs.us-cert.gov/ All NSF CAE programs, particularly UIUC (NCSA), CMU, Purdue, Tulsa, and workshops [32] Morris CC 2-year program http://www.ccm.edu/academics/degrees/infosecurity.aspx Stevens concentration programs http://www.stevens.edu/ses/graduate/cybersecurity-grad.html West Point info assurance curriculum http://www.westpoint.edu/crc/SitePages/Home.aspx CyberWatch http://www.cyberwatchcenter.org/ Shodor http://www.shodor.org/ GWU CS Policy Institute http://www.cspri.seas.gwu.edu/ C3 "Cool Careers" workshops http://www.edtechpolicy.org/cyberk12/c3workforcecareers.html	Focus on fundamentals [8], [28], [36] Transfer [5], [7], [19] , [18], [34] Problem-based, collaborative, inquiry-based, experiential Teaching by "front lines" field leaders Evaluation is key; assessment by accomplishment Need to differentiate the goals of 2-year, 4-year and postgraduate programs Dealing with proliferation of standards Creating career awareness and prestige	Rutgers Professional Science Master's program http://psm.rutgers.edu/	Concentrator and non-concentrator-focused lecture courses Online courses - AP Computer Science MOOC [38] - DIMACS VCTAL modules: 4) internet privacy http://dimacs.rutgers.edu/VCTAL/computational.html Virtualization, simulation, gamification: [45] Stewart, Humphries, Andel. "Developing a virtualization platform for courses in networking, systems administration and cyber security education." Competitions [13] Conklin. "Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course."	Journal of Homeland Security Education Information Systems and Security Education Journal [44] Spidalieri, "One Leader at a Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat." 2013. http://pellcenter.salvereginablogs.com/files/2013/04/One-Leader-at-a-Time-FINAL.pdf [1] ACM/IEEE-CS Joint Task Force on Computing Curricula. 2013. Computer Science Curricula 2013. ACM Press and IEEE Computer Society Press. http://www.acm.org/education/CS2013-final-report.pdf ACM Computing Curricula http://csta.acm.org CSTA Cyber standards http://csta.acm.org/Advocacy_Outreach/Other/CSTACyberStandards.pdf [47] DHS Homeland Security Advisory Council, Cyber Skills Taskforce Report. Fall, 2012. http://www.dhs.gov/sites/default/files/publications/HSAC%20Cyber%20Skills%20Report%20-%20Final.pdf

Category 4: Other Students Receiving Cyber-Security-Enhanced Education	NSA CryptoKids HS/ College programs http://www.nsa.gov/kids/student/index.shtml USAF Cyber-patriot http://www.uscyberpatriot.org/ BSA Cyber Chip Merit Badge http://www.scouting.org/scoutsource/boyscouts/advancementandawards/meritbadges/cyber_chip.aspx ICCSP (UIUC Cyber Scholars Program) http://www.iti.illinois.edu/education/illinois-cyber-security-scholars-program-icssp UMD Pre-college workshops/camps http://cyber.umd.edu/education/pre-college; UMD REU's and Undergrad honors pgm http://cyber.umd.edu/education/undergrad [34] Security Injections @ Towson: http://cis1.towson.edu/~cssecinj/	Attention, memorableness, generating excitement Targeting specific age groups	AP courses Epidemiology US Armed Forces educational system	Training Modules Camps / workshops NSF February 2014 [32]	NICE Cybersecurity in K-12 http://csrc.nist.gov/nice/Sept2011-workshop/presentations/Thursday/Thurs_Cuny_NICE_K-12_092211.pdf iKeepSafe c3 matrices http://www.ikeepsafe.org/educators/more/c3-matrix/ DIMACS Privacy Module http://dimacs.rutgers.edu/VCTAL/Modules/PrivacyModuleDraftAugust2012-PDF.pdf [10] College Board: New Course and Exam – AP Computer Science: Principles to Launch in Academic Year 2016-2017. http://www.collegeboard.com/html/computerscience/