Toward CAE-CDE 4Y Designation through Curriculum Modernization of a Traditional Computer Science Undergraduate Program

Wei Wei
wei@uhcl.edu

T. Andrew Yang
yang@uhcl.edu

Sadegh Davari
davari@uhcl.edu

Kewei Sha
sha@uhcl.edu

Johanna Jacob
JacobJ5081@UHCL.edu

Department of Computing Sciences
University of Houston-Clear Lake
Houston, TX 77058

Abstract

Defending the cyberspace calls for troops of qualified cyber professionals (including architects, developers, managers, and various cyber operators) who possess the necessary set of knowledge and skills. Higher education institutions, especially computing related fields such as Computer Science, share the responsibility in producing the future cyber defense workforce. This paper describes our attempt in revamping a traditional CS curriculum at a teaching-oriented university in order to fulfill the Center of Academic Excellence in Cyber Defense Education (CAE-CDE) designation requirements. In details, we discuss how we overcome several resource constraints without sacrificing program quality. We also explain and illustrate the design rationale and process, which may interest other institutions with similar goals. Furthermore, we examine relevant frameworks and guidelines and show how they could be useful in our and other similar efforts.

Keywords: Cybersecurity, CAE-CDE, Curriculum, Framework, Computer Science

1. INTRODUCTION

Defending our cyberspace and information systems against various types of attacks and threats is an increasingly challenging task. The challenges are even more severe for smaller businesses and organizations whose resources are scarce and cybersecurity talents are often lacking. The constantly evolving nature of cyber threats makes traditional, passive control mechanisms ineffective, especially with the fast growth and spread of emerging technologies such as Virtualization, Blockchains, Internet of Things (IoT), etc. A recent BitDefender report predicted that, by 2020, financial losses caused by cybercrime will reach $2 trillion while the

cybersecurity market will exceed $100 billion (Nuresan, 2016).

Lack of skills and technical knowledge has been identified as the biggest barrier to successfully implementing cyber defense; this applies to both organizations and the nation as a whole. As suggested in the first-ever Federal Cybersecurity Workforce Strategy by the White House (Donovan, Cobert, Daniel, & Scott, 2016), one of the key initiatives is to collaborate with academic institutions to develop guidance for cybersecurity core curriculum and allow colleges and universities to expand their course offerings. Higher education institutions across the nation ought to take this new challenge and opportunity to modernize their computing degree programs in order to help the nation's response to these challenges, by preparing cyber-aware professionals to meet the nation's increasing demand for cybersecurity talents. Though cybersecurity is in nature an interdisciplinary field, computing related college programs are at the core of preparing future cybersecurity professionals, especially cyber operators. In a radio talk given by Allan Paller (Temin, 2016), he took a long-term view of our cybersecurity preparedness and pointed out that all sectors, especially government, are in desperate needs of cybersecurity professionals who can "do the technical things" such as security coding, penetration testing, and network forensics. Those programs that only offer survey courses can only produce "admirers" rather than "fixers" of our problems. Therefore, what we need in our education programs are solid computing knowledge plus advanced hands-on skills. A competent cybersecurity practitioner should have fundamental understanding of computing and mathematics, and they should also be proficient with programming and problem solving, all of which are already addressed in a Computer Science (CS) undergraduate program with solid quality.

The Center of Academic Excellence in Cyber Defense Education (CAE-CDE) is a program co-sponsored by National Security Agency (NSA) and the Department of Homeland Security (DHS). The goal is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise for the nation. Earning this designation is a rigorous process and the requirements have been clearly stated. So far, only about 200 U.S. institutions out of over 5,300 colleges and universities have obtained that designation (Dawson, Wang, & Williams, 2018). In the state of Texas, there are eight CAE-CDE Four-Year Baccalaureate Education (CAE-CDE 4Y) designated institutions, all of which have a doctoral program in a cybersecurity related fields. Out of the eight institutions, none of them is teaching-oriented. This is a void because nationwide, 53% of the CAE-CDE 4Y institutions are teaching-oriented schools. In addition, only two out of the eight designated programs are housed in Computer Science (CS) while others are affiliated with Information Systems (IS) or Information Technology (IT) programs. The nature of those programs, therefore, are either less hands-on or lack programming components. Therefore, we argue that more CS-affiliated CAE-CDE 4Y cybersecurity programs with focus on cyber operation in teaching-oriented institutions are needed in Texas. Furthermore, only one of the eight programs is in Houston. This puts Houston in a very disadvantageous position strategically in terms of defending our cyberspace. Houston, as the 4th largest city in the U.S., is an important center for many industries including transportation, medical, aerospace, and oil and gas. With so many facilities, sea ports, airports, and industrial plants intensively packed in the region, it is easy to imagine that Houston is a prime target of various cyber-attacks. The Houston region demands a sufficient supply of cybersecurity workers to protect its computing systems and critical infrastructures against prospective cyber-attacks. Therefore, we advocate that more Houston-based higher education institutions should invest in CS-affiliated CAE-CDE designated programs.

The University of Houston-Clear Lake (UHCL) is a Hispanic-serving institution located in the high tech community of Clear Lake, near NASA Johnson Space Center. Computer Science is the largest program in the College of Science and Engineering at UHCL with a total enrollment of 466. The CS program at UHCL has been accredited by the Accreditation Board of Engineering and Technology (ABET) since 2002. Our CS program has developed and offered certain cybersecurity related courses such as Computer Security; in addition, security related topics have been woven into courses such as Operating Systems and Computer Systems Administration. After analyzing the current situation with cybersecurity educational programs in the Greater Houston area, we have set our goal to obtain the CAE-CDE 4Y designation through revamping our existing CS undergraduate curriculum. The merits of our initiative were well recognized and awarded with a NSF CyberCorps grant. The purpose of this paper is to share what we have learned through the process with

educators from fellow institutions who are also interested in developing security-integrated CS programs.

The rest of the paper is organized as follows. In Section 2, we introduce our general approach and the rationales behind this effort. In Section 3, we provide more details on the execution of that approach. In Section 4, we investigate the relationship between our proposed approach and a newly published cybersecurity undergraduate curriculum guideline. We then conclude in Section 5.

2. THE GENERAL APPROACH

Obtaining the CAE-CDE 4Y designation is a long journey. Our ultimate goal is to house a cybersecurity program in our CS department that will be CAE-CDE designated. The barriers to overcome along this journey include but are not limited to: (1) Resource constraints: this is especially important for small teaching-oriented institutions like us. The resources include teaching and research faculty and staff, and institutional facilities/infrastructure. (2) Program sustainability: Once the program is created, will it attract enough enrollments? Can our graduates meet the local market needs/demands? (3) Ever-changing environment: The forefront of cybersecurity battlefield evolves constantly; therefore, what are required of our future professionals need to reflect the changes. This kind of volatility requires our implementation approach to be adaptive and responsive. (4) Program quality: In addition to meeting the criteria for the designation, the content of the program also needs to conform to some other standards/guidelines for purposes such as accreditations and future compatibility. In order to deal with the identified challenges, we have strategized and come up with the high-level solutions as summarized in Table 1.

Challenges & Solutions
C1. Resource constraints • Utilize and/or modify existing course structure and courseware to come up with the most cost-effective course path; • Design/create new courseware in modular structure for plugability and extensibility; • Utilize courseware that are made publically available through other research/education projects.
C2. Program sustainability • Survey among current CS student body; • Establish/maintain partnership with local industry/businesses; • Community outreach programs to attract future students.
C3. Changing environments • Infuse faculty research into curriculum design; • Stay informed of knowledge and skills of market demands.
C4. Program quality • Conform to the CAE-CDE designation requirements; • Build courseware based on CAE-CDE Knowledge Units (KU); • Mapping to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) (Newhouse, Keith, Scribner, & Witte, 2017); • Potentially conform to the Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (CSEC2017 Joint Task Force, 2017); • Potentially conform to the ABET accreditation criteria for cybersecurity (ABET, 2017).

Table 1 High Level Solution Summary

In this paper, we focus the discussion of our solutions on two of the challenges, i.e., the resource constraints and program quality.

3. CURRICULUM REVAMPING

Despite the ever-increasing demands for qualified cybersecurity professionals, cybersecurity as a mature academic discipline is yet to be legitimized (Raj & Parrish, 2018). In addition, many established cybersecurity academic programs are at master or doctoral degree level. Design and implementation of undergraduate degree programs in cybersecurity remain challenging for several reasons. First, cybersecurity is interdisciplinary in nature and entails a wide range of topics and areas. There is no clear and universally-accepted definition of such a program with clearly defined objectives and scope. Second, even when we narrow down the scope to a specific sub-area, there is no abundance of well-established programs for new-comers to model after. Third, for a new cybersecurity program to be housed under existing computing related disciplines, it is a challenge for the curriculum to remain within the degree plan's credit hour limit. In our practice, our general principle is to take well into consideration of our existing CS curriculum and, in the most cost-effective way, conform to known standards and best practice without sacrificing the quality of the designed program. With meeting the CAE-CDE designation requirements

as the ultimate goal, the overall process of revamping our CS curriculum is illustrated in Figure 1. Note: KU in the diagram stands for 'knowledge unit'.

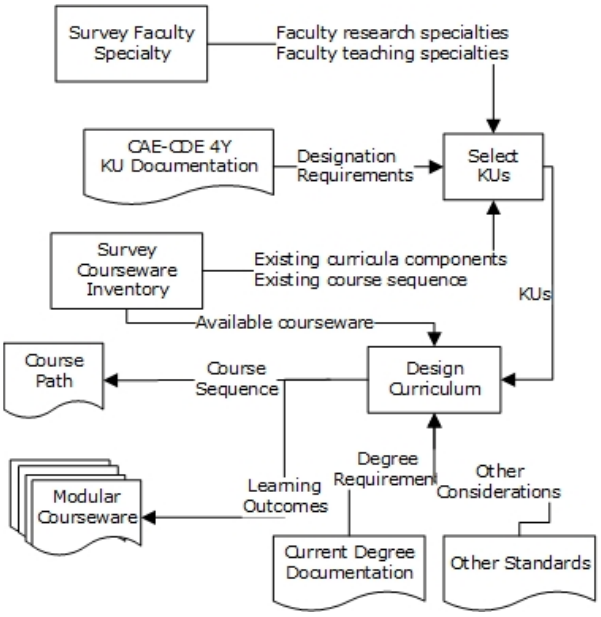

Figure 1 Overall Curriculum Design Process

Preliminary Preparation

The whole process starts with a comprehensive survey of all existing courses in our current CS undergraduate program. The purpose is to investigate what cybersecurity related instructional components are already in our curriculum. We collected and analyzed all course syllabi. We then complied a master list of all courses and/or course components that are cybersecurity related, including student learning outcomes and covered topics. In addition, we also collected the specialties of our faculty. This is important because it allows us to choose a focus area that is most relevant and feasible. Based on our survey, the CS department currently has faculty members who specialize in networking and network security. This allows us to have a better focus in the Knowledge Unit (KU) selection in later stages of the curriculum development.

Understanding the Requirements

Another important step is to familiarize ourselves with the CAE-CDE 4Y designation process and requirements. Note that NSA and DHS recently published a revised set of KUs which are to be effective for the 2019 application cycle starting on Oct 1st, 2018. The discussions in this paper refer to the new set of KUs.

The requirements of CAE-CDE designation is organized using KUs and Specializations. A typical KU consists of a minimum list of required topics to be covered and one or more learning outcomes. In addition, when applicable, the connection between the KU and the NICE Cybersecurity Workforce Framework (NCWF) at the Categories level is also indicated. Also, more than a dozen of specializations are defined by other agencies. A specialization can be designated when the necessary KUs are covered to deliver the desired set of skills and abilities. Usually, a specialization demands a combination of some technical and non-technical core KUs plus some optional KUs.

The amount of information related to the designation process and relevant frameworks is vast and complex. Our team has spent substantial amount of time to survey and understand relevant documents. These efforts not only generated publications (Jacob, Wei, Sha, Davari, & Yang, 2018) but also helped ensure that our curricular design is valid and feasible.

KU Selection

Based on our preliminary study results, we have decided that, in order to revamp our CS program to meet the CAE-CDE 4Y designation KU requirements, we will implement the following 22 KUs as shown in Table 2.

3 Cybersecurity Foundational KUs:
• Cybersecurity Foundations (CSF) • Cybersecurity Principles (CSP) • IT Systems Components (ISC)
5 Technical Core KUs:
• Basic Cryptography (BCY) • Basic Networking (BNW) • Basic Scripting and Programming (BSP) • Operating Systems Concepts (OSC) • Network Defense (NDF)
14 Optional KUs:
• Databases (DAT) • Network Technology and Protocols (NTP) • Data Structures (DST) • Digital Forensics (DFS) • Policy, Legal, Ethics, and Compliance (PLE) • Linux System Administration (LSA) • Network Forensics (NWF) • Cyber Crime (CCR) • Cybersecurity Ethics (CSE) • Intrusion Detection/Prevention Systems (IDS) • Network Security Administration (NSF) • Secure Programming Practices (SPP) • Web Application Security (WAS) • Wireless Sensor Networks (WSN)

Table 2 Selected Knowledge Units

Curriculum Course Path Design

Based on selected KUs to cover, we aggregated a list of required learning outcomes and topics that was compared against the master list of existing courseware. Then we arranged the courses (existing or new) in a path so that: (1) Courses that already cover required topics are put into the path with meaningful sequences in between. (2) Courses with the necessary augmentations (with CAE-CDE designation required KUs) are organized into the path. The augmentation can be done through incorporating modular units into existing instructional activities. (3) New courses are to be designed to bridge the gap between designation requirements and existing curriculum. These new courses can fit in the degree plan as potential electives. The course path can be found in Figure 2 presented in the Appendix. The curriculum prepares students with traditional CS courses in terms of mathematics, programming, and other knowledge and skills. In addition, various security elements, especially those related to network security, are already embedded in the curriculum. Following this path, students in our CS undergraduate program can fulfill their degree requirements within the allowed credit hours with a concentration on cybersecurity, more specifically, focusing on Network Security.

In Table 3, we illustrate where and how each of the selected KUs would be fulfilled in the course path.

KUs	Source of Coverage
CSF	Cyber Attacks and Defense*
CSP	Cyber Attacks and Defense*
ISC	Multiple computing courses
BCY	Cyber Attacks and Defense*
BNW	Network Protocol
BSP	Multiple programming courses
OSC	Operating Systems
NDF	Network Security*
DAT	Design of Databases
NTP	Network Protocol
DST	Data Structures
DFS	Computer Forensics
PLE	Cyber Attacks and Defense*
LSA	Computer System Administration
NWF	Network Forensics*
CCR	Cyber Attacks and Defense*
CSE	Cyber Attacks and Defense*
IDS	Network Security*
NSF	Network Security*
SPP	Cyber Attacks and Defense*
WAS	Cyber Attacks and Defense*
WSN	Network Security*

*New course

Table 3 KU Coverage in Designed Curriculum

In the CAE-CDE designation requirements, each KU is defined with a set of desired learning outcomes. Therefore, with the selected KUs for our proposed curriculum, we have a combined list of learning outcomes to achieve and assess. Instructional content to deliver these learning outcomes are allocated in different courses—existing or new. Due to space limit, we cannot include the complete list of learning outcomes. But we hereby provide a small sample to demonstrate how they are mapped to curricular components. Note that a learning outcome may be matched to more than one course because the underlying concepts/abilities are important and should be reiterated throughout the curriculum. In addition, the mapping could be done at course module level instead of course level.

KUs	Learning Outcomes	Mapped to
BSP	Demonstrate proficiency in the use of a programming language to solve complex problems in a secure and robust manner	CS1, CS2, Data Structure
NDF	Explain how network defense tools (firewalls, IDS, etc.) are used to defend against attacks and mitigate vulnerabilities.	Network Security*
NWF	Analyze and decipher network traffic,	Network Forensics*
OSC	Identify and describe basic security issues of operating systems.	Operating Systems, Cyber Attacks and Defense*

*New course

Table 4 Sample Mapping between Learning Outcomes and Curricular Components

Courseware Design and Implementation

With the ultimate goal of applying for CAE-CDE 4Y designation, our courseware design focuses on filling the gap between what already exist and what more are needed, in terms of topics to cover and learning outcomes to achieve.

New content is designed and then organized in a modular fashion. Modules and submodules can be organized into a new course as seen in the Appendix, or plugged into existing courses for the purpose of augmentation. Each submodule may contain one or more instructional units (either lecture or lab). A central repository is created to accommodate all implemented courseware units that are annotated and labeled. This not only helps organize the efforts of applying for the

designation in the future, but also makes the created content searchable and discoverable. Other faculty members could incorporate certain units into their own teaching; this certainly enhances the likelihood of building/reinforcing a CS program that will cultivate our future computing professionals with the necessary security mindset. In Table 5, we show the general structure of a new course called Cyber Attacks and Defense, which has Data Structures as prerequisite. This is designed to be the introductory cybersecurity course for CS undergraduate students. The content covers various technical and non-technical KUs/topics. The technical content is a combination of lectures and hands-on labs. The technical skills and abilities acquired enable the students to become cyber operators, strengthened by their solid computing and programming skills. The non-technical content is equally important because it is the opportunity to broaden the horizon of a typical CS student in terms of what cybersecurity entails. It will help break them free from the typical "hacker" mindset and realize that there are many human, organizational, legal, societal, and other factors in safeguarding our cyberspace. As an introductory course, this covers a wide range of topics but at a rather shallow depth. For instance, many of the network related topics will be revisited with much more technical details down the course path. Making this the introductory course to CS students can also help them get a taste of cybersecurity as a profession and decide whether they want to pursue further.

Module 1. Security Fundamentals
• Submodule 1: Security Concepts and Principles • Submodule 2: Security Management • Submodule 3: The Cybersecurity Profession and Careers
Module 2. Security Threats and Countermeasures
• Submodule 1: Security Threats • Submodule 2: Cyber Crimes • Submodule 3: Countermeasures • Submodule 4: Safeguard the IT Infrastructure • Submodule 5: Introduction to Cryptography
Module 3. Network Security
• Submodule 1: Networking basics • Submodule 2: Network Protocols • Submodule 3: Network Administration Basics • Submodule 4: Network Security Basics
Module 4. Software Security
• Submodule 1: Software Vulnerabilities and Security • Submodule 2: Low-level Attacks and Defense • Submodule 3: Secure Programming • Submodule 4: Web-based System Security
Module 5. Cloud Security
• Submodule 1: Cloud Computing Fundamentals • Submodule 2: Cloud Security Basics

Table 5 Course Design of Cyber Attacks and Defense

In Table 6 and Table 7, we list some sample instructional units to demonstrate the content of the other two new courses, Network Security and Network Forensics. Both courses are organized in the Module→Submodule→Instructional Units structure as well.

Submodule: <u>Network Defense Mechanisms</u>
• Network Access control • DMZs/Proxy Servers • Implementing Firewalls and VPNs • Application-layer security: HTTPS • Network-layer security: IPSec
Submodule: <u>Network defense Hands-on</u>
• Network sniffing using Wireshark • Implementing IPSec • Setting up honeypots • Securing a web server

Table 6 Instructional Units of Network Defense

Submodule: <u>Network Technique and Forensics</u>
• Proxies and Forensics • Firewalls and Forensics • NIDS & NIPS and Forensics • VPN and Forensics • Router and Forensics
Submodule: <u>Network Forensics Hands-on</u>
• Tcpdumping with the libpcap library • Sniffing wireless traffic with Wireshark • Packet sniffing and analysis with NetworkMiner • Malware identifying with YARA • Evidence acquisition with SNORT • Collect and analyze log files with Splunk

Table 7 Instructional Units of Network Forensics

As a general rule, we intend to include labs as much as possible to enhance the learning experience by allowing the students to "see security in action". Developing a series of labs is very resource intensive. In addition to designing cost, the investment into long-term recurring

maintenance of the necessary infrastructure alone may become cost prohibitive for a small institution. Therefore, we seek reusing lab components created by other educational efforts. For example, we plan to utilize results from the SEED project (Du, 2011) to support our lab needs as much as possible. For more advanced courses such as Network Security and Network Forensics, we need to develop our own labs and we will share those with the community. As seen in Table 6 and Table 7, both courses include substantial amount of hands-on activities that employ various networking security techniques and tools.

4. CONFORMING TO OTHER GUIDELINES

The National Initiative for Cybersecurity Education (NICE) acknowledges the cybersecurity workforce deficiency and has published the NICE Cybersecurity Workforce Framework (NCWF). (Newhouse et al., 2017). This framework organizes cybersecurity work in a hierarchy of Categories->Specialty Areas->Work Roles in order to provide a cybersecurity work taxonomy and common lexicon. Mapping has been created between the NCWF content to the CAE-CDE KUs. Therefore, even we do not map our curriculum content directly to the NCWF framework, the connection is indirectly achieved through conforming to the CAE-CDE requirements.

The National Security Agency and the Department of Homeland Security have been the early advocates of collaborating with higher education institutions to educate future cybersecurity professionals through Centers of Academic Excellence (CAE). Gradually, computing related programs everywhere are implementing some sort of cybersecurity programs at various scales with different focus. As we see this as a positive trend that can help us with the cybersecurity hiring crisis, we also see the needs of uniformity and control. Until recently, there has been a void of an academic curriculum guideline for cybersecurity.

Several major international computing societies including the Association for Computing Machinery (ACM), the IEEE Computer Society (IEEE CS), the Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC), and the International Federation for Information Processing Technical Committee on Information Security Education (IFIG WG) have formed a joint task force—the CSEC 2017 Joint Task Force on Cybersecurity Education (JTF). The mission of the task force is to develop comprehensive and flexible curricular guidance in cybersecurity education that will support future program development and associated educational efforts at the post-secondary level (CSEC2017 Joint Task Force, 2017). Compared to the NICE Cybersecurity Workforce Framework (NCWF) (NIST, 2017), this curriculum guideline is more relevant because the intended audience is "faculty in computing-based disciplines at academic institutions". The center piece of this guideline is the CSEC thought model as seen in Figure 2.

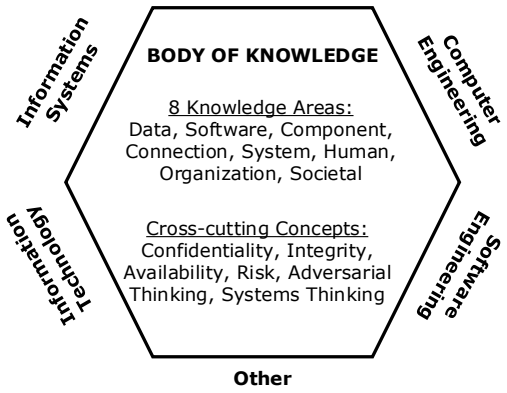

Figure 2. CSEC Thought Model (CSEC2017 Joint Task Force, 2017)

This model uses three dimensions to define the curricular framework. The eight knowledge areas provide a high level structure of cybersecurity related content. The crosscutting concepts "provide an organizational schema for interrelating knowledge". The disciplinary lens represents the computing disciplines that can house a cybersecurity program. Note that this guideline was published after our initial curriculum design. However, our design fits nicely into the model. To be more specific, we take the Computer Science perspective and have instilled the cross-cutting concepts throughout. In terms of the eight knowledge areas, our curriculum provides a comprehensive coverage of all, with more emphasis on Connection Security.

In this guideline, Knowledge Areas (KAs) are used as basic organizing structure. Each KA covers multiple Knowledge Units. A knowledge unit may be placed under multiple knowledge areas since the content from various knowledge areas may overlap. For example, the knowledge unit Data Privacy is contained in Data Security, Human Security, Organizational Security, and Society Security. This is understandable because data privacy, as an integral component of data

security, has its unique Human, Organization, and Societal impact and implications. Another example is that the knowledge unit System Thinking applies to both System Security and Software Security knowledge areas. It is important to know that the knowledge units here do not correspond to the KUs used for CAE-CDE designation, though some similarities are observed. Furthermore, each knowledge unit encompasses multiple topics. These topics are particularly useful for academia since they define the essential curricular content. In this aspect, the guideline could play an important role in unifying instructional efforts across various cybersecurity programs. The identified topics also come with students learning outcomes.

This guideline also addresses the importance of bridging the gap between cybersecurity in higher education and the hiring needs. This is vital because, in general, graduates often have deficiencies in specific knowledge and skills to fit into future operational environment, either technical ones such as network defense or non-technical ones such as regulatory compliance. Therefore, it is important to connect cybersecurity educational guidelines with certain cybersecurity workforce frameworks. This guideline makes such an effort by referring to the NCWF framework. To be specific, at a high level, the Topics and Learning Outcomes are meant to be linked to the Knowledge, Skills, and Abilities (KSA) of the NCWF framework. These KSAs are what's required to perform certain work roles. Knowledge is the body of information needed to do so. Skills call for physical manipulation of tools and/or application of frameworks, processes. Ability refers to competence to do something. Therefore, we should expect to see many action verbs at application level or above in those learning outcomes. Instances of those action verbs include Apply, Use, Practice, etc. In order to see if this is indeed the case, we investigated the Learning Outcomes in more details. There are eight knowledge areas, and altogether 137 learning outcomes. As shown in Table 8, we have summarized the percentages of action verbs corresponding to the hierarchies in the Bloom's Taxonomy (knowledge, comprehension, application, analyzing, evaluation, and synthesizing).

Bloom's Taxonomy	Sample Action Verbs	%
Knowledge	Identify, List	9.5%
Comprehension	Describe	29.9%
	Explain	25.5%
	Discuss	19.7%
	Paraphrase, summarize	3.6%
Application	Implement	1.5%
Analyzing	Differentiate	3.6%
	Compare	1.5%

Table 8 Learning Outcomes Action Verbs Used

Other than the small portion of action verbs that are hard to categorize (5.2%), majority (more than 75%) of the learning outcomes stay at the Comprehension level, which assess students' understanding of new material. Only about 7% of learning outcomes actually require students to apply new knowledge or skills, or to analyze something as part of critical thinking. There are no learning outcomes focus on Evaluation and Synthesizing. This finding suggests that most of the learning still stays at Know-What level; a little Know-Why exists and the Know-How part is obviously missing. We argue this calls for attention if equipping our students with necessary skills and abilities is an important goal.

The cybersecurity program we are designing is housed in Computer Science. The nature of our program is technical oriented with a focus on network security. Therefore, we expect our graduates to possess sufficient technical skill sets. These requirements will be indicated clearly in our learning outcomes. For instance, for the topic of network security, we expect students to be able to "use typical network administration tools". For the topic of software security principles, we expect students to be able to "apply the learned software security best practice in software development." Operational skills, both technical and non-technical, can be acquired in hands-on labs, case studies, and internship opportunities. Throughout the curriculum, we need to keep in mind the importance of preparing our students to be more market-ready. To that end, while keeping the integrity and rigor of higher education, we could incorporate more content borrowed from training and professional development in cybersecurity. As to exactly where the boundary should be drawn, it is an interesting question for us in academia to answer through practice.

5. CONCLUSIONS

Our project aims at revamping the current CS undergraduate curriculum in order to meet the CAE-CDE 4Y designation requirements. As a regional teaching-oriented institution, we find no prior attempts for us to model after. Therefore, in our exploratory efforts, we seek feasible approaches to overcome various barriers

especially the resource constraints. In our curricular design and implementation, we try to reuse existing quality curricular components plus new ones related to various aspects of cybersecurity. We also emphasize the importance of including enough hands-on activities to acquire the must-have skills and abilities. We have made plans to assess proposed instructional components and evaluate how they could serve to fulfill specified learning outcomes at both course and program levels. The assessment procedure and results are beyond the scope of this paper, but we will share them with the community once they are ready. Furthermore, we conducted comprehensive studies of many relevant frameworks and guidelines to ensure the quality of our design. This is an ongoing project and we will continue to explore, learn, and in turn share our lessons with the community.

ACKNOWLEDGMENTS

This research has been supported by the National Science Foundation (under grant #1723596) and by the National Security Agency (under grant # H98230-17-1-0355).

6. REFERENCES

ABET. (2017). ABET Seeks Feedback on Proposed Accreditation Criteria for Cybersecurity Academic Programs. Retrieved from http://www.abet.org/blog/news/abet-seeks-feedback-on-proposed-accreditation-criteria-for-cybersecurity-academic-programs/

CSEC2017 Joint Task Force. (2017). *Cybersecurity Curricula 2017 Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. Retrieved from https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Dawson, M., Wang, P., & Williams, K. (2018). The Role of CAE-CDE in Cybersecurity Education for Workforce Development. In *Information Technology-New Generations* (pp. 127-132): Springer.

Donovan, S., Cobert, B., Daniel, M., & Scott, T. (2016). Strengthening the Federal Cybersecurity Workforce. Retrieved from https://www.whitehouse.gov/blog/2016/07/12/strengthening-federal-cybersecurity-workforce

Du, W. (2011). SEED: hands-on lab exercises for computer security education. *IEEE Security & Privacy, 9*(5), 70-73.

Jacob, J., Wei, W., Sha, K., Davari, S., & Yang, T. A. (2018, July 30-August 2). *Is the NICE Cybesecurity Workforce Framework (NCWF) Effective for a Workforce Comprising of Interdisciplinary Majors?* Paper presented at the The 16th International Conference on Scientific Computing, Las Vegas, USA.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework SP 800-181. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

NIST. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Retrieved from https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

Nuresan, R. (2016). Cybersecurity market to exceed $100 billion by 2020; financial losses caused by cybercrime to reach $2 trillion. Retrieved from https://businessinsights.bitdefender.com/cybersecurity-market-cybercrime-losses

Raj, R. K., & Parrish, A. (2018). Toward Standards in Undergraduate Cybersecurity Education in 2018. *Computer, 51*(2), 72-75.

Temin, T. (2016). Alan Paller: Federal progress in cybersecurity. Retrieved from http://federalnewsradio.com/federal-drive/2016/06/alan-paller-federal-progress-in-cybersecurity/

APPENDIX: Proposed Course Path

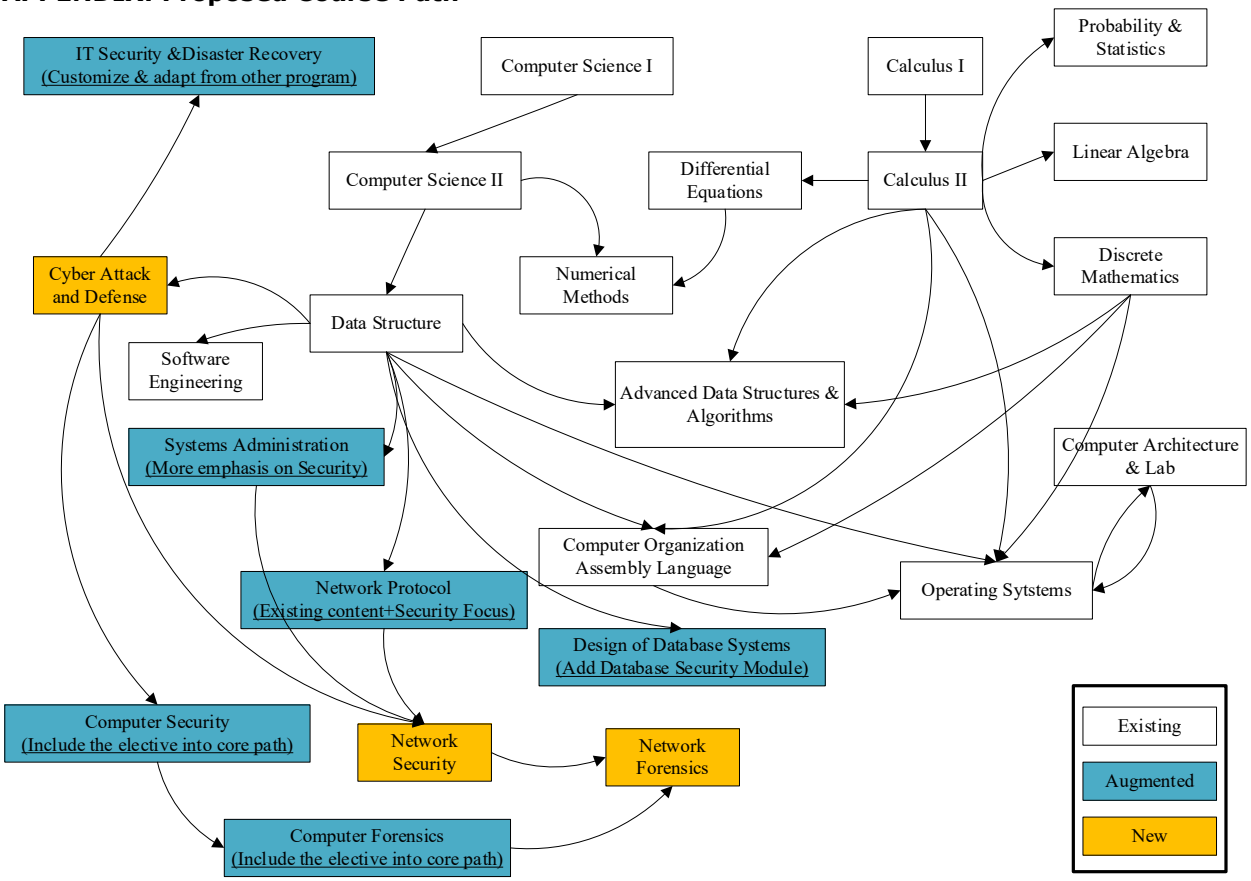

Figure 3 Proposed Course Path