Cybersecurity Associate Degree Program Curriculum

Dr. Melissa Stange
ACM CCECC
Lord Fairfax Community College
Middletown, VA, USA
mstange@lfcc.edu

Dr. Cara Tang
ACM CCECC
Portland Community College
Portland, OR, USA
cara.tang@pcc.edu

Cindy Tucker
ACM CCECC
Bluegrass Community & Techincal College
Lexington, KY, USA
cindy.tucker@kctcs.edu

Dr. Christian Servine
ACM CCECC
El Paso Community College
El Paso, TX, USA
cservin1@epcc.edu

Dr. Markus Geissler
ACM CCECC
Cosumnes River College
Sacramento, CA, USA
geisslm@CRC.losrios.edu

***Abstract*— The spotlight is on cybersecurity education programs to develop a qualified cybersecurity workforce to meet the demand of the professional field. The ACM CCECC (Committee for Computing Education in Community Colleges) is leading the creation of a set of guidelines for associate degree cybersecurity programs called Cyber2yr, formerly known as CSEC2Y. A task force of community college educators have created a student competency focused curriculum that will serve as a global cybersecurity guide for applied (AAS) and transfer (AS) degree programs to develop a knowledgeable and capable associate level cybersecurity workforce. Based on the importance of the Cyber2yr work; ABET a nonprofit, non-governmental agency that accredits computing programs has created accreditation criteria for two-year cybersecurity programs.**

Keywords—Higher Education, Curriculum, Cybersecurity, Associate Degree, Community, Junior, & Technical College, CSEC2Y, Cyber2yr

I. Introduction

Cybersecurity is the practice of protecting computer systems from cyber-attacks, physical or digital damage to hardware, software, and unauthorized use of technology. With growth of “smart devices” and the Internet of Things (IoT), cybercrimes are also growing and the attacks are becoming more innovative, giving the cybersecurity industry a more prominent role in the daily lives of every person. Cybersecurity is often only associated with computers, however, it extends to a wide array of technologies like mobile devices, televisions, cars, cameras, cryptocurrency, identity theft, e-government, and many more.

Cybersecurity has only recently emerged as an identifiable discipline, and cybersecurity degree programs are still relatively young. CSEC2017 defines cybersecurity as: “A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management” [1]. International research and advisory firm Gartner Inc. predicts worldwide security spending will hit $96.3 billion in 2018, an 8% increase in just one year [3]. A recent survey from Nationwide Mutual Insurance Company found that 58% of business owners with up to 299 employees had been victims of a cyber-attack [4]. The U.S. Bureau of Labor Statistics (BLS) predicts that jobs for information security analysts will grow by 28% between 2016 and 2026 [2].

While Cybersecurity is emerging as a separate discipline, it is also an important element of all computing programs. Curriculum content in creating and maintaining secure computing environments is a critical component in associate-degree computing programs of all types. Almost every career path open to a computing student encompasses some aspect of security. System administrators and engineers must be able to properly design, configure, and maintain a secure system; programmers and application developers must know how to design and build secure, fault-tolerant software systems from the bottom up; web specialists must be capable of assessing risks and determining how best to reduce the potential impact of breached systems; user support technicians must be knowledgeable in security concerns surrounding desktop computing; and project managers must be able to calculate the cost/benefit tradeoffs involved with implementing secure systems. It is the responsibility of faculty to ensure that students are well prepared for the cybersecurity challenges they will inevitably encounter in their careers as computing professionals.

II. Bachelor Cybersecurity curriculum development

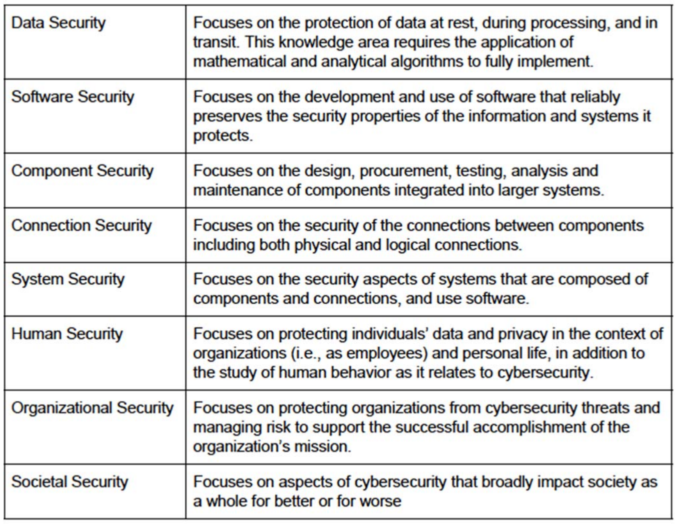
A. Curriculum Development Background

In 2015 a Joint Task Force on Cybersecurity Education (JTF) kicked off with the purpose of developing a comprehensive curricular guide in cybersecurity education that would support future program development and associated

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE
978-1-7281-5092-5/19/$31.00 ©2019 IEEE

educational efforts. The JTF was a collaboration between major international computing societies consisting of IEEE Computer Society (IEEE CS), Association for Computing Machinery (ACM), Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and the International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). The JTF grew out of the foundational efforts of the Cyber Education Project (CEP).

After much community involvement such as public reviews, presentations at professional conferences such as Women in Cybersecurity (WiCyS) 2016, CyCon US 2016: International Conference on Cyber Conflict, CUBERSEC: European Cybersecurity Forum 2016, and the 2016 & 2017 Colloquium for Information Systems Security Education (CISSE), in December of 2017, the Joint Task Force on Cybersecurity Education published Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (CSEC2017) [1], representing a new discipline in ACM's Computing Curricula Series. The eight knowledge areas and their definitions from CSEC2017 at the bachelor degree level are shown in Fig. 1.



Data Security	Focuses on the protection of data at rest, during processing, and in transit. This knowledge area requires the application of mathematical and analytical algorithms to fully implement.
Software Security	Focuses on the development and use of software that reliably preserves the security properties of the information and systems it protects.
Component Security	Focuses on the design, procurement, testing, analysis and maintenance of components integrated into larger systems.
Connection Security	Focuses on the security of the connections between components including both physical and logical connections.
System Security	Focuses on the security aspects of systems that are composed of components and connections, and use software.
Human Security	Focuses on protecting individuals' data and privacy in the context of organizations (i.e., as employees) and personal life, in addition to the study of human behavior as it relates to cybersecurity.
Organizational Security	Focuses on protecting organizations from cybersecurity threats and managing risk to support the successful accomplishment of the organization's mission.
Societal Security	Focuses on aspects of cybersecurity that broadly impact society as a whole for better or for worse

Fig. 1: CSEC2017 Knowledge Areas [10]

III. Associate Cybersecurity Curriculum Development

A. *CCECC and Cyber2yr Task Force*

The ACM Committee for Computing Education in Community Colleges (CCECC) serves and supports community and technical college educators in all aspects of computing education, with a focus on producing curriculum guidelines for associate-degree programs in ACM-recognized computing disciplines. Based on the work of the CSEC2017 Task Force, the CCECC is leading creation of a similar set of guidelines for cybersecurity programs at the associate-degree level, called Cyber2yr.

The Cyber2yr (Cybersecurity 2-year) task force consist of 10 community college educators who have been working collaboratively since April 2018 to create Cyber2yr, formerly known as CSEC2Y. Two drafts, known as StrawDog and IronDog were presented and available for public feedback between February and August 2019. The curriculum was presented at the Association of Computing Machinery (ACM) SIGCSE Technical Symposium, Community College Cyber Summit (3CS), ACM International Innovative Technology in Computer Science Education (ITiCSE), IEEE NoVA Education Technical webinar, and the 2nd Annual Virginia Cybersecurity Education Conference. The task force is incorporating collected feedback on the curriculum, creating rubrics, and collecting program examples from a variety of Cybersecurity programs at the associate level, with the goal of final delivery in January 2020.

B. *Cyber2yr Design*

All eight of the Knowledge Areas (KAs) from CSEC2017 were selected for inclusion within Cyber2yr. However, not all Knowledge Units (KUs), nor all topics within the KUs from CSEC2017 were appropriate for associate level programs. Each KU was identified with one of three indicators. The three indicators used were all, meaning every associate degree program should include, some, meaning that a few may include and none, meaning that no associate level program would include. The knowledge units identified as being in some were relabeled as "Supplemental" and the areas that all should include were relabeled as "Essential". Of the topics included in CSEC2017, 35.2% were essential and 42.4% were found to be supplemental. The remaining 22.4% of topics were found to be not appropriate at the associate degree level, as seen in Fig. 2. Fig. 3 shows the distribution of KA topics in Table 1 at the associate level.

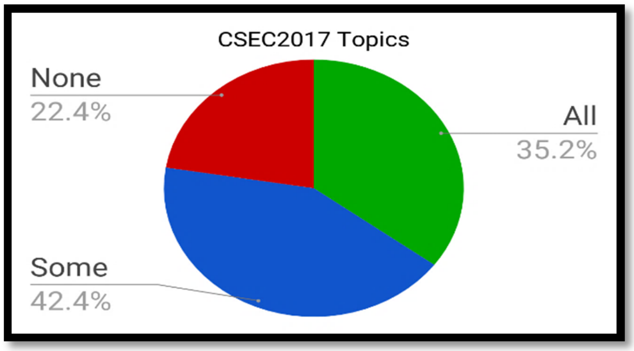


Fig. 2: Distribution of CSEC2017 Knowledge Areas for Cyber2yr [11]

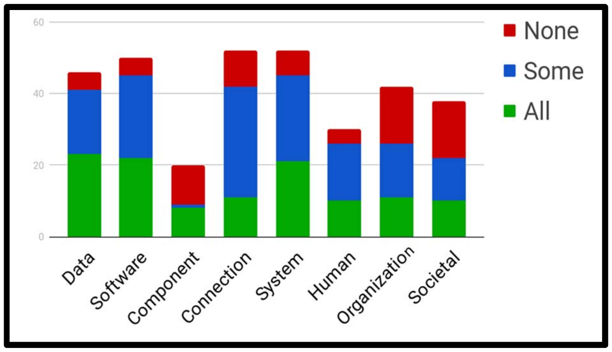


Fig. 3: Distribution of CSEC2017 Topics for Cyber2yr [11]

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

The curriculum StrawDog and IronDog drafts [10,15] had the Essential KAs and KUs as listed within Table 1. The majority of these KUs are also found within the supplemental items, excluding component design, component Procurement, component reverse engineering, physical interfaces and connectors, hardware architecture, business continuity and Incident management, and cybersecurity planning. Additional units within the supplemental include physical media, analytical tools, security program management, personal security, data privacy, and information storage security.

Table 1: KAs and KUs for StrawDog & IronDog

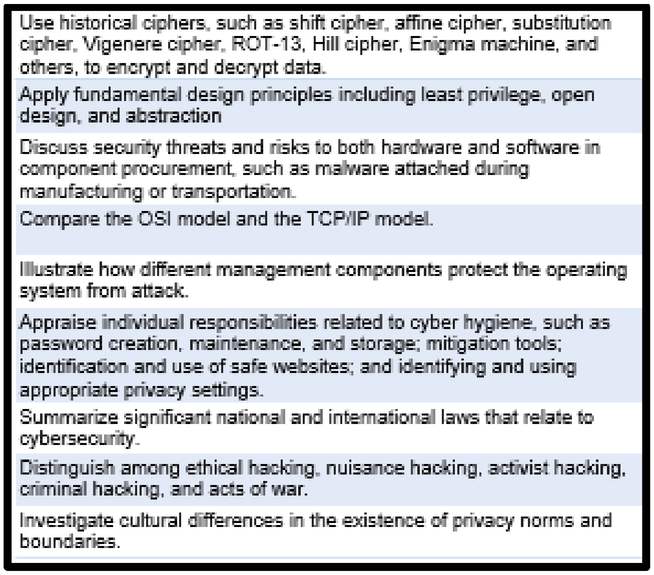
Knowledge Area	Knowledge Units
Data Security	Cryptography, Digital Forensics, Data Integrity And Authentication, Access Control, Secure Communication Protocols, Cryptanalysis, Data Privacy, And Information Storage
Software Security	Fundamental Principles, Design, Implementation, Analysis And Testing, Deployment And Maintenance, Documentation, And Ethics
Component Security	Component Design, Component Procurement, Component Testing, And Component Reverse Engineering
Connection Security	Hardware And Physical Component Interfaces And Connectors, Distributed Systems Architecture, Network Architecture, Network Implementations, Network Services, And Network Defenses
System Security	System Access, System Management, System Thinking, Systems Control, System Testing, And Common System Architectures
Human Security	Identity Management, Social Engineering, Personal Compliance With Cybersecurity Rules/Policy And Social Norms, Awareness And Understanding, Personal Data Privacy And Security, And Usable Security And Privacy
Organizational Security	Management, Security Governance And Policy, Systems Administration, Cybersecurity Planning, Business Continuity And Incident Management
Societal Security	Cybercrime, Cyber Law, Cyber Ethics, Cyber Policy, And Privacy

There are six main themes, referred to as cross-cutting concepts within Cyber2yr, which are woven throughout the guidelines, including

- Confidentiality, rules that limit access to system data and information to authorized persons;
- Integrity, assurance that the data and information are accurate and trustworthy;
- Availability, the data, information, and system are accessible;
- Risk, potential for gain or loss;
- Adversarial thinking, a process that considers the potential actions of the opposing force working against the desired result;
- Systems thinking, a process that considers the interplay between social and technical constraints to enable assured operations.

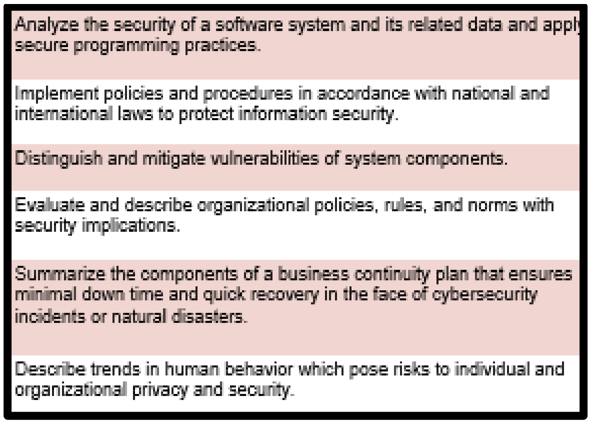
C. Competencies, Blooms, and Frameworks

Cyber2yr further differs from CSEC2017 by focusing on student achievement in terms of competencies (Fig. 5) and learning (Fig. 4) outcomes instead of topics. Each KA within the framework has three to five high-level competencies and associated learning outcomes. The competencies follow the definition presented in Modelling Competencies for Computing Education beyond 2020: A Research Based Approach to Defining Competencies in the Computing Disciplines [16]: “Competency integrates knowledge, skills, and dispositions and is context-situated.” Knowledge (“know-that”) refers to “mastery of core concepts and content knowledge.” Skills (“know-how”) are “qualities that people develop and learn over time with practice and through interactions with others.” Dispositions (“know-why” and “know-yourself”) include “attitudinal, behavioral, and socio-emotional qualities of how disposed people are to apply knowledge and skills to solve problems.” Context is the setting in which competencies manifest, the “authentic situations related to problems/issues and aspects of work.” The student learning outcomes were added to provide more detailed student expectations than the competencies alone and may serve as a course or lesson learning outcomes. The learning outcomes focus on what students can do over merely what students may know. Both the competencies and learning outcomes are expressed using action verbs from Bloom’s Revised Taxonomy.



Use historical ciphers, such as shift cipher, affine cipher, substitution cipher, Vigenere cipher, ROT-13, Hill cipher, Enigma machine, and others, to encrypt and decrypt data.
Apply fundamental design principles including least privilege, open design, and abstraction
Discuss security threats and risks to both hardware and software in component procurement, such as malware attached during manufacturing or transportation.
Compare the OSI model and the TCP/IP model.
Illustrate how different management components protect the operating system from attack.
Appraise individual responsibilities related to cyber hygiene, such as password creation, maintenance, and storage; mitigation tools; identification and use of safe websites; and identifying and using appropriate privacy settings.
Summarize significant national and international laws that relate to cybersecurity.
Distinguish among ethical hacking, nuisance hacking, activist hacking, criminal hacking, and acts of war.
Investigate cultural differences in the existence of privacy norms and boundaries.

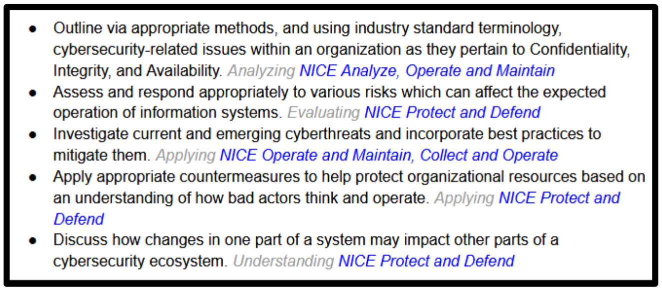
Fig. 4: Sample Subset of Learning Outcomes [11]



Analyze the security of a software system and its related data and appl secure programming practices.
Implement policies and procedures in accordance with national and international laws to protect information security.
Distinguish and mitigate vulnerabilities of system components.
Evaluate and describe organizational policies, rules, and norms with security implications.
Summarize the components of a business continuity plan that ensures minimal down time and quick recovery in the face of cybersecurity incidents or natural disasters.
Describe trends in human behavior which pose risks to individual and organizational privacy and security.

Fig. 5: Sample Subset of Competencies [11]

The Cyber2yr curriculum guidelines have also been influenced by the CAE-CD 2Y 2019 knowledge units (requirements of the NSA and DHS National Centers of Academic Excellence in Cyber Defense [12], and the NICE Cybersecurity Workforce Framework [13] and the ACM Code of Ethics [14] as seen in Fig. 6. Mathematics has not been addressed at a specific level within the curriculum guidelines due to the diversity within the regional and degree design. The Cyber2yr recommendation is that each program include sufficient mathematics to meet the cybersecurity outcomes for the program.



- Outline via appropriate methods, and using industry standard terminology, cybersecurity-related issues within an organization as they pertain to Confidentiality, Integrity, and Availability. Analyzing NICE Analyze, Operate and Maintain
- Assess and respond appropriately to various risks which can affect the expected operation of information systems. Evaluating NICE Protect and Defend
- Investigate current and emerging cyberthreats and incorporate best practices to mitigate them. Applying NICE Operate and Maintain, Collect and Operate
- Apply appropriate countermeasures to help protect organizational resources based on an understanding of how bad actors think and operate. Applying NICE Protect and Defend
- Discuss how changes in one part of a system may impact other parts of a cybersecurity ecosystem. Understanding NICE Protect and Defend

Fig. 6: Cross-Cutting Competencies with Blooms & Nice Framework [11]

D. *Importance of Cyber2y*

Due to the high number of cybersecurity job openings currently and expected by 2021 as seen in Fig. 7 from the Aspen Cybersecurity group, employers are going to need to rely on a cybersecurity workforce without a bachelor or higher degree. This is where Cyber2yr becomes critical in defining the essential knowledge, skills, and dispositions of any cybersecurity professional upon entering into the workforce or continuing into an upper level undergraduate program.

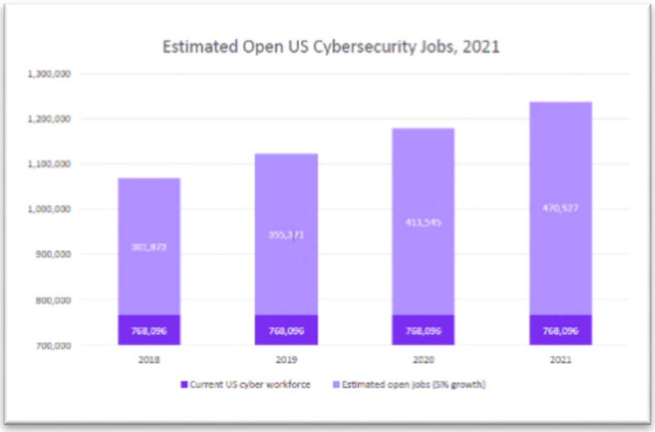


Fig. 7: Estimated Open U.S. Cybersecurity Jobs [17]

E. *Next Steps for Cyber2y*

The Cyber2y task force will continue to refine the learning outcomes and competencies, while building a cross-walk to other frameworks, collecting cybersecurity program examples to be shared on the CCECC website, and finalize the Cyber2y Curriculum Guide by January 2020 and available on the Association for Computing Machinery (ACM) Committee for Computing Education in Community Colleges (CCECC) website located at http://ccecc.acm.org/.

Acknowledgment

The CCECC committee would like to thank the Association for Computing Machinery (ACM) for supporting this work of the CCECC committee. The Cyber2yr task force members for their hard work and dedication. The CCECC committee national and international advisors and the volunteer curriculum draft reviewers. Thanks to the CSAB and CAC advisors with ABET.

References

[1] ACM, IEEE, AIS, and IFIP (2017) Cybersecurity Curricula 2017. https://cybered.hosting.acm.org/wp.

[2] Bureau of Labor Statistics. (2016). Information Security Analyst. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-1.

[3] Gartner, Inc. (2018). Global security spending to reach $96.3bn in 2018. https://www.gigabitmagazine.com/big-data/global-security-spending-reach-963bn-2018-gartner.

[4] Nationwide Mutual Insurance Company. (2017). Nearly Half of Business Owners Have Been Victims of Cyberattacks — But Didn't Know It. https://www.nationwide.com/personal/about-us/newsroom/press-release?title=100917-cyber-security.

[5] Parrish, A & Sobiesk, E. (2016). Developing ABET Criteria for Undergraduate Cybersecurity Programs. Frontiers in Education 2016 Proceedings. 978-1-5090-1790-4/16.

[6] Accreditation Board for Engineering and Technology (ABET). (2017). ABET seeks feedback on Proposed Accreditation Criteria for Cybersecurity Engineering Programs. Retrieved from https://www.abet.org/abet-seeks-feedback-on-proposed-accreditation-criteria-for-cybersecurity-engineering-academic-programs/.

[7] Accreditation Board for Engineering and Technology (ABET). (2018). ABET Approves Accreditation Criteria for Undergraduate Cybersecurity Programs. Retrieved from https://www.abet.org/abet-approves-accreditation-criteria-for-undergraduate-cybersecurity-programs/.

[8] Bradshaw, M (2018). TU at the forefront of Cybersecurity. Retrieved from https://www.towson.edu/news/2018/abetaccreditation.html.

[9] United States Naval Academy. (2018). Naval Academy Cybersecurity Program Receives ABET Accreditation. Retrieved from https://www.usna.edu/NewsCenter/2018/09/NAVAL%20ACADEMY%20CYBERSECURITY%20PROGRAM%20RECEIVES%20ABET%20ACCREDITATION.php.

[10] ACM CCECC. (2018). Cybersecurity Curricular Guidance for Associate Degree Programs. Retrieved from https://ccecc.acm.org/files/publications/CYBER2YR-StrawDog.pdf.

[11] Tang, C., Tucker, C., Sevin, C., Geissler, M., & Stange, M. (2019). Shaping Curricular Guidelines for Associate-Degree Cybersecurity Programs. Proceedings of the ACM SIGCSE'19. 978-104503-0000-0/11806. https://doi.org/10.1145/3287324.3287516.

[12]]NSA and DHS, Centers of Academic Excellence in Cyber Defense (CAE-CD) 2019 Knowledge Units, https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf

[13] National Initiative for Cybersecurity Education (NICE). 2017. NICE Cybersecurity Workforce Framework. NIST Special Publication 800-181. DOI: https://doi.org/10.6028/NIST.SP.800-181.

[14] ACM. (2018). ACM Code of Ethics and Professional Conduct. https://www.acm.org/code-of-ethics

[15] ACM CCECC. (2019). Cybersecurity Curricular Guidance for Associate Degree Programs. Retrieved from https://ccecc.acm.org/files/publications/CSEC2Y-IronDog.pdf.

[16] Stephen Frezza, Mats Daniels, Arnold Pears, Åsa Cajander, Viggo Kann, Amanpreet Kapoor, Roger McDermott, Anne-Kathrin Peters, Mihaela Sabin, and Charles Wallace. 2018. Modelling Competencies for Computing Education beyond 2020: A Research Based Approach to Defining Competencies in the Computing Disciplines. In Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE '18 Companion), July 2-4, 2018, Larnaca, Cyprus. ACM, New York, NY, USA, 27 pages. https://doi.org/10.1145/3293881.3295782.

[17] Aspen Cybersecurity Group (2018). Principles for Growing and Sustaining the Nations Cybersecurity Workforce.https://assets.aspeninstitute.org/content/uploads/2018/11/Aspen-Cybersecurity-Group-Principles-for-Growing-and-Sustaining-the-Nations-Cybersecurity-Workforce-1.pdf?_ga=2.131709199.1031855205.1564591048-412768538.1560292992.