Bridging the disconnect within Cybersecurity Workforce Supply Chain

Olatunji Osunji
College of Business, Innovation, Leadership and Technology Marymount University
Arlington, VA U.S.A
o0o34411@marymount.edu

Abstract—Within the Cybersecurity workforce supply chain, there continues to be a disconnect between the undergraduate curriculum and industry skill demand. The cybersecurity workforce framework of the National Initiative for Cybersecurity Education can serve as one of the tools to bridge this disconnect. Borrowing from the learnings in the training of students in medical school, this paper performs a qualitative literature review on some of the existing efforts to develop the cybersecurity workforce. By exploring the integration of the cybersecurity workforce framework and the curriculum guideline of the Joint Task Force on Cybersecurity Education, it recommends the introduction of Entrustable Professional Activities and mandatory apprenticeship as part of the curriculum guideline. The Entrustable Professional Activities could be based on workforce tasks defined by NICE and cybersecurity graduates will be expected to demonstrate capability to perform those activities. Industry participation is required across all levels of the supply chain.

Keywords—Apprenticeship, Cybersecurity, Entrustable Professional Activities, Joint Task Force, NICE, Workforce

I. INTRODUCTION

The ability of academia, industry, and government to develop a highly-skilled cybersecurity workforce supply chain is important for the wellbeing of the citizens [1]. A joint survey conducted by McAfee and The Center for Strategic and International Studies revealed that, about 77 percent of employers feel that the educational curriculum is not effectively preparing students for the cybersecurity profession [2]. Findings indicate that the cybersecurity skill gap exists because the industry demands for cybersecurity professionals outweigh the supply of highly, technically skilled (HTS) cybersecurity graduates [3][4]. As of April 2021, there are half a million unfilled cybersecurity positions within the United States and the current supply of qualified professionals is just about half of that [5].

Two initiatives that have been directed towards improving this skill shortage are the National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework (NICE Framework) and the curriculum guideline produced by the Joint Task Force (JTF) on Cybersecurity Education. Both initiatives represent a public-private collaborative effort to address the work force gaps - from different, but complementary ends.

While the cybersecurity professions protect the wellbeing of individuals in the digital world, two professions that are hands-on and perform similar duties of securing people's wellbeing, but in the physical world are the medical and military professions. The military has traditionally been responsible for defending and protecting the nation from attacks launched on air, land, sea and space and they are specially trained for this purpose. The medical profession continues to improve the quality of training provided to students towards a medical degree. This paper looks at how the medical profession has approached an identified skill gap within the education and training curriculum of physicians. handling the training challenge within its curriculum.

The problem that this study hopes to address is the disconnect between educational curriculum and the industrial demand for highly skilled professionals amid initiatives like NICE and JTF guidelines. The research question is, what can the cybersecurity learn from the workforce supply chain of the medical profession and how can the NICE framework and JTF guidelines be adapted to improve the quality of cybersecurity graduates?

This research focuses on undergraduate cybersecurity degrees and uses qualitative review of documents centered around NICE framework, JTK guidelines and training requirements for Medical students. The paper proposes mandatory inclusion of apprenticeship into the curriculum of undergraduate cybersecurity programs and the apprenticeship can be based on tasks listed for a chosen work role as defined in the NICE framework.

This section is followed by a review of the work done by NICE, JTK and the medical field. Section III covers the analysis and discussion, followed by recommendations and conclusion.

II. METHODOLOGY

Our cybersecurity workforce supply chain is placing an over-emphasis on theory within cybersecurity education programs [3]. To address the research questions, a qualitative method based on grounded theory was adopted. From information hidden in data, grounded theory aims to construct a new theory [6], models or conceptual framework [7]. Applying grounded theory, this research reviews the hidden data within NICE framework, JTK curriculum guideline and the approach to managing skill gap challenges

observed among medical students going into residency. Conceptual clarity was obtained by inquiring into relationships between the works of JTK and NICE.

A. Joint Task Force on Cybersecurity Education

In 2015, a JTF on Cybersecurity Education, consisting of the Association of Computing Machinery (ACM), Institute of Electrical and Electronics Engineers -Computer Society (IEEE CS) , Association for Information Systems Special Interest Group on Security (AIS SIGSEC) and International Federation for Information Processing (IFIP) was formed. One of their goals was to develop a curriculum guideline that aligns cybersecurity academic programs at the undergraduate level with industry needs [8]. This led to the classification of cybersecurity as a new discipline under computing. The developed curriculum guideline was based on the existing five computing discipline earlier established in 2005 - Computer Engineering; Computer Science; Information Systems; Information Technology; and Software Engineering as foundation [9]

The guideline adopted the concept of knowledge units (KU) - multiple related topics, learning outcomes(LO) – expectation of what learners should know or be able to do, and of knowledge areas (KA) - combination of knowledge units and learning outcomes . Essential, it uses a knowledge framework where students are required to demonstrate proficiency in each KA through attainment of the LO. A review of the guideline [8] reveals that learning outcomes are placed within Bloom's taxonomy level of understanding and applying. Bloom's taxonomy is a classification of education goals [10].

With the realization that the traditional model based on KA has not produced graduates that meet industry demand, JTK in 2020 adopted a competency model (CC2020) for cybersecurity and other computing disciplines [11]. It acknowledges that in order to meet industry demand, knowledge- "know-what"; skills- "know-how"; dispositions -"know-why"; and tasks should be integrated into the undergraduate curriculum. However, it pointed out that the necessary resources for skills and disposition transfer are not readily available within most academic settings and there are indications that industry is avoiding training of recent graduates of computing related degrees- including cybersecurity. While it offers the suggestion for inclusion of work-study and cooperative programs to make up for skills transfer, it raised concerns that students in work-study may take longer time to graduate. As part of the competency tools that can be adopted, CC2020 mentions the i Competency Dictionary (iCD), which originated from Japan. It has a task diagnostic criteria and corresponding Diagnostic Levels of L0-L4, which is a good fit to evaluate learner's performance in completing task(s).

B. The National Initiative for Cybersecurity (NICE)

In recognition of the criticality of the workforce gap and continuation of the efforts of his predecessor, President Obama established NICE in 2010 [1]. The NICE frameworks, until the version published in 2017 (NIST Special Publication 800-181) were made of three components: categories, specialty areas, and work roles. Each work role represents sets of standard knowledge, skills, and abilities (KSA) required of learners to complete defined tasks [12]. The framework also uses a competency model, hence it emphasizes the need for right behavioral attitude – in addition to KSA.

In 2020, a revision was published which discontinued the use of categories, specialties and need for abilities. Instead it uses knowledge, skills, and tasks as its building blocks. Task defines actions necessary to achieve digital risk management objectives, while skills and knowledge are capabilities required to be able to perform individual tasks.

The NICE framework views competencies as a way for industry to assess learners [13] - which are undergraduates in this research. It illustrated two approaches for the workforce to map competencies, knowledge, skills, and tasks. Approach 1 is competencies based on a defined set of tasks, for which assessment can be based on lab work (a hands-on approach). In Approach 2, competency is based on skills and knowledge, and employers assess learners through credentials (degrees or certifications). Approach 2 appears to be what is obtainable within our educational system, which has focused more on the theoretical part and laid more emphasis on knowledge at the expense of skills.

C. Readiness for Medical Residency

While duration of physician education and training differ widely from one nation to another, one common denominator within the education and training of physicians is the inclusion of clinical clerkship (CC) in medical schools [14]. CC places medical students in a hospital setting where they learn by observing and performing activities in preparation for residency programs. However, documented literature reveals that performance gaps exist as medical students progress from medical school to residency [15]. This led the Association of American Medical Colleges (AAMC) to publish a list of 13 Core Entrustable Professional Activities (Core EPAs) [15]. These are tasks that medical school graduates are expected to have the knowledge, skills and disposition to perform on their first day of residency, without direct supervision, regardless of specialty choice.

Entrusting requires each student to be trustworthy [16][17] and trustworthiness is about honesty and diligence in performing duties [18]. To be entrusted, a medical student is expected to develop and be competent in performing the EPAs [19]. Trustworthiness is a virtue that is also expected of cybersecurity professionals since they are required to protect, defend and respond to cyber incidents. Based on revelation from several researches, [20] reported that beyond the CC, acting internship rotations have proved to be an effective means of preparing students to demonstrate their ability to perform these EPAs. The internships provide the opportunity for supervising physicians to observe students and offer feedback through workplace-based assessment. One of the goals of American Medical Association (AMA) was to transition medical education to a competency based education [21]. Nothing is implied since the EPAs align the assessment process with learners' action and supervisors'

observation. Evaluation is based on how well learners apply knowledge to tasks. Stages of how well a learner progresses in competency is referred to as milestones. Even though it is a niche concept, [22] cited previous research reported an increase in EPA adoption and that it will likely influence the direction of AMA's competency based medical training globally.

D. Past Recommendations

Some of the previous recommendations include: cybersecurity education and training programs should be designed to be hands-on and involve applied learning [23]. Apprenticeship, internship, or work-study options are means of tackling the hands on skills issue in cybersecurity education [11][24]. Apprenticeships and Work-study should be part of the cybersecurity program's curriculum [2][25]. On the faculty side, [26] argued for the need for continuous professional development among academia.

III. Discussions and Analysis

This section details the analysis of the literature review and based on grounded theory attempts to highlight information rooted in the documents reviewed.

A. Findings

Literature reviewed as revealed the convergence of approaches towards a competency based framework between the NICE framework and JTK curriculum guideline. In addition, collaboration exists between academia, public and the private sector towards a workforce common goal. However, the reluctance of industry to invest in training recent graduates, with the expectation that they should come equipped with necessary skills at time of graduation, calls for concern. This paper is of the opinion that more participation from industry at every stage of the workforce supply chain will be required to tackle the workforce gap. Recommendations from various stakeholders (as highlighted in previous section) focuses on the need to incorporate apprenticeship, internship, or work-based learning into the cybersecurity curriculum. However, it is still optional for most cybersecurity degree programs. In addition to this, several cybersecurity programs have focused on students graduating on time (fast track programs), thereby increasing the quantity of graduates that are supplied into the workforce at the expense of quality. A comparison of the JTK and NICE approach is shown in Table I.

TABLE I. NICE and JTF Comparison

	JTK - Cybersecurity	NICE
1	Workforce gap from supply view	Workforce gap from demand view
2	Approach workforce issues from an education curriculum lens.	Approach workforce issues from task statements/job description.
3	Competency as an educational goal.	Competency as a means for industry to assess learners.
4	Competency = Knowledge, Skill, disposition in task execution	Competency = knowledge, skills, and behavior in task execution.
5	Learning outcome falls within Bloom's taxonomy of Understanding and Applying	Task expectation mostly falls at a minimum Bloom's taxonomy of Applying.

The educational systems that feed into the workforce supply chain produce graduates with credentials – which are meant to establish learner's competency. According to [11], industry can use combinations of certifications and degrees as credentials. Likewise, an option stated in the NICE framework is for industry to assess competencies using credential - approach 2 from the previous section. Based on the grounded theory approach used, this report sees a need for the tasks (if any) defined under competency based curriculum to synchronize with those defined under the NICE framework (workforce expectation). Without this synchronization of tasks, the curriculum developed using a competency framework may not achieve its purpose. This is one of the conceptual clarities represented in Fig. 1, which is the basis for further discussion.

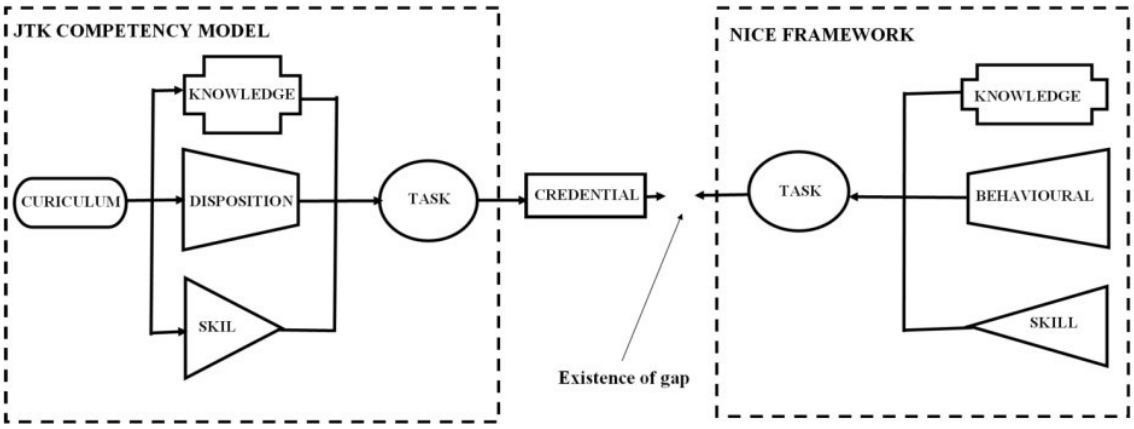

Fig. 1. Combining NICE Framework and JTF Competency Framework

B. Discussion

For an illustration, the NICE framework has a Work role titled - *cyber operator*. The role has 44 knowledge areas, 26 skills with 26 tasks assigned to it [26]. These skills and tasks are not one to one mapping. A student interested in taking up a position in this role is expected to demonstrate hands-on ability to perform these 26 tasks.

A review of the knowledge areas revealed that students are expected to have taken not less than twelve undergraduate courses spanning areas like Networking, Operating System, Cryptography, Malware Analysis, Vulnerability Management among others computing courses. These course works should lay the foundation for the 44 knowledge areas and part of 26 skills. Most of the skills require usage of tools which may not all be available in colleges, hence industry exposure is required – preferably under the supervision of a highly technical cybersecurity professional. Further analysis of the 26 tasks reveals that they are placed with a minimum Bloom's taxonomy level of applying. This is not in sync with JTK guidelines, which initially aim at a level between understanding and applying for the undergraduate curriculum.

In answering the research question: *what can cybersecurity learn from the medical field?* The training of physicians involves years of combined education and training which exposes them to the hospital environment through mandatory clinical, internship and residency. One can only imagine the rate of casualties if the hospitals are manned by inadequately trained physicians - supposing clinical trainings are optional. The Core EPAs were introduced to bridge competency gaps in the supply chain of the medical profession. Just like the medical profession requires competent individuals who can be entrusted with tasks aimed at saving lives, the cybersecurity profession needs competent individuals who can be entrusted with not only protecting the confidentiality, integrity, and availability of data, but also harm to lives of individuals that can arise from a cybersecurity incident. Attacks on critical infrastructure like the Colonial Pipeline in the U.S.A and Ukraine power grid hack in mid-winter readily come to mind. This paper is of the strong opinion that the mandatory inclusion of hands- on training in curriculum and establishment of Core EPAs equivalent are two offerings that cybersecurity can adapt from the medical field.

C. How can the NICE framework and JTF guidelines be adapted based on these learnings?

This is answered below as part of the recommendation.

D. Recommendations

1. The undergraduate curriculum should consist of two parts- education and training. The education should focus more on knowledge- "know what" and foundation for disposition - "know why", while training develops the skills - "know how" and core of disposition in performing identified tasks.

2. Apprenticeship should be incorporated into undergraduate cybersecurity curriculum and made mandatory - under training part of the curriculum. This should be in collaboration with industry and a supervisor assigned for each student. Such training can be designed as a six month training during or after the third year (for U.S colleges), This will cover summer and fall semester or spring and summer of the third year. During this period, students will not be required to be in school, instead they will be under the supervision of an industry professional.

3. Industry should be involved earlier in the cybersecurity workforce supply chain. Industry needs to take ownership and partake in the training of undergraduate students before graduation and not after. This starts from the curriculum development, especially the training part of the curriculum. The early involvement of industry ensures that students are exposed to the expectation of industry demand.

4. Using the roles and tasks defined by NICE, an equivalent of Core EPAs should be setup and incorporated into the cybersecurity curriculum. Unlike the medical field which has only 13 EPAs, the EPAs for cybersecurity curriculum should vary based on work role. The learning outcome will be demonstration of capability to perform the tasks and the iCD Diagnostic Level can be adopted for assessing learners by supervisors.

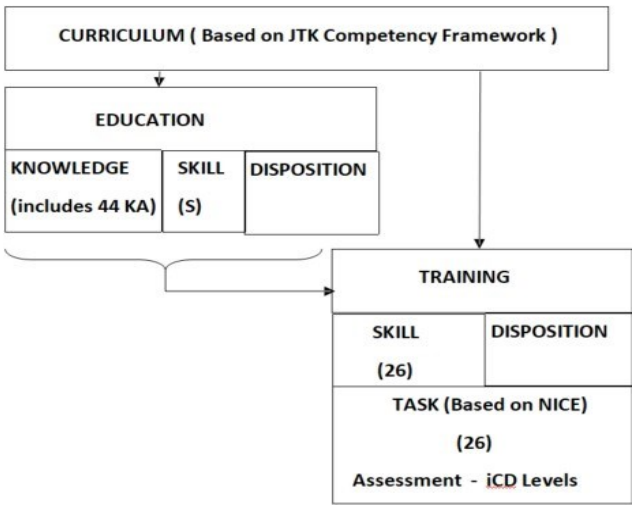

Fig. 2. Curriculum design based on NICE Framework and JTF Competency Framework

To design and incorporate the apprenticeship program into undergraduate curriculum, the task description from the NICE framework should be fed into the competency framework guideline of JTK. This ensures integration between the two competency frameworks. The task will help define the learning outcome expected of a learner and this will be the focus of the apprentice program. A sample conceptual design for a learner choosing cyber operator as a work role is shown in Fig. 2. The education part of the curriculum will have embedded in it, courses which will include the 44 knowledge areas and some aspect of the 26 skills (S) – since academia does not have the necessary

resources and environment to cover all 26 skills. The 26 tasks will be the EPAs for such learners who would be expected to demonstrate capability to perform the tasks after completion of a mandatory apprenticeship. iCD [11][27] has a sample Diagnostic Criteria for Task assessment ranging from L0 – "*No knowledge or experience*" to L4 – "*Can instruct others*". An adaptation of iCD Diagnostic level for this scenario is shown in Table II and may be used for evaluating the learner.

TABLE II. ASSESSMENT LEVEL BASED ON ICD

Diagnostic Level	**Diagnostic Criteria**
L0	Has knowledge based on education.
L1	Can carry out tasks with supervision.
L2	Can carry out tasks with minimal support.
L3	Can carry out tasks independently.
L4	Can instruct others.

Another student interested in the *Cyber Defense Analyst* work role [28], will have a different EPAs based on the NICE 34 task assigned to this role.

It is worth noting that these recommendations come with some concerns. One is an increase in length of study due to the mandatory apprenticeship. The other is who finances the training of learners? Making apprenticeship mandatory does not have to increase the time spent in school. As an example, in the United States, a Bachelor's degree in Computer Science or Cybersecurity with mandatory apprenticeship or internship can still be structured into the normal four year program. The curriculum should be developed to include courses that matter. While the quantity and time to produce cybersecurity graduates are important factors, quality is the critical factor needed. Arrays of "fast track" cybersecurity degrees, most of which have no training component, will widen the skills gap, instead of bridging it.

In the area of finance, this is where the industry has a major role to play. For this period, say six months of apprenticeship, students will be working for the company while also learning. Technically, the student should be paid.

IV. CONCLUSION AND FUTURE WORK

A. Limitation

Literature collected and reviewed for this research is limited to those available online and in the English language. In addition, it uses existing work of NICE and JTF frameworks as foundation.

B. Conclusion

The workforce disconnect can be solved through effective collaboration and joint ownership by academia and industry, government. JTK and NICE have set a precedent for collaboration among academia, public and private sector, however, the industry needs to be involved earlier in the training stage of the supply chain of cybersecurity workforce. This paper has reviewed the works of JTK and NICE on cybersecurity workforce development. Borrowing from the learnings in the medical field, it has recommended apprenticeship or internship be mandatory for undergraduate programs and sets of Entrustable Professional Activities based on NICE's task be defined and applied as learning outcome. It also recommended that industry should actively be involved all through the supply chain of workforce development and not only after graduation. Since most of the tools that need mastery are either developed in the industry or being used extensively in the industry, technology giants like Microsoft, IBM, AWS, Oracle Google, Government agencies and federal contractors should invest in training regardless of interest in employing the students or not.

C. Future Work

Future research hopes to explore how best to develop EPAs using NICE taxonomies and structure the training part of the curriculum with a view to translate competency framework to improved learning outcome. A pilot of this concept may be necessary as part of future work to understand its practicality and effectiveness.

REFERENCES

[1] NIST. "National Initiative for Cybersecurity Education, National Cybersecurity Workforce Framework, ver. 1.0," 2013. [Online]. Available: https://www.nist.gov/file/359276

[2] Center for Strategic and International Studies (CSIS). "Hacking the Skills Shortage," 2016 [Online]. Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf.

[3] W. Crumpler and J. A. Lewis. "The Cybersecurity Workforce Gap," 2019. [Online]. Available: http://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf

[4] Concordiam. "The Urgent Need for Cyber Security Workforce Development," Journal of European Security and Defense Issues Volume 10, Issue 4. 2020. [Online]. Available: https://perconcordiam.com/perCon_V10N4_ENG.pdf

[5] NIST. "Cybersecurity Supply/Demand Heat Map. Cyberseek" 2021. [Online]. Available: https://www.cyberseek.org/heatmap.html

[6] K. Charmaz. "Special Invited Paper: Continuities, Contradictions, and Critical Inquiry in Grounded Theory," International Journal of Qualitative Methods 16, 1 (dec 2017), 160940691771935. [Online]. Available: https://doi.org/10.1177/1609406917719350

[7] A. Bryant. "Grounded theory and grounded theorizing: Pragmatism in research practice," New York, NY: Oxford University Press. 2017.

[8] Joint Task Force on Cybersecurity Education. 2018. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Association for Computing Machinery, New York, NY, USA

[9] Association for Computing Machinery (ACM). Computing Curricula 2005. 2005. [Online]. Available: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2005-march06final.pdf

[10] Association for Computing Machinery (ACM). "Bloom's Revised Taxonomy," 2021. [Online]. Available: http://ccecc.acm.org/assessment/blooms

[11] Association for Computing Machinery (ACM). "Computing Curricula 2020 CC2020 Paradigms for Global Computing

Education. 2020," [Online]. Available: DOI: https://dl.acm.org/doi/book/10.1145/3467967

[12] W. Newhouse, S. Keith, B. Scribner, and G. Witte. "National Initiative for Cybersecurity Education (NICE). Cybersecurity Workforce Framework, NIST Special Publication 800-181" 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-181

[13] R. Petersen, D. Santos, K. A. Wetzel, M. C. Smith, and G. Witte. "Workforce Framework for Cybersecurity (NICE Framework)," 2020 [Online]. Available: https://doi.org/10.6028/NIST.SP.800-181r1

[14] Y. M. Mowery. "A primer on medical education in the United States through the lens of a current resident physician. Annals of translational medicine," 3(18), 270. 2015. [Online]. Available: https://doi.org/10.3978/j.issn.2305-5839.2015.10.19

[15] Association of American Medical Colleges (AAMC). Core Entrustable Professional Activities for Entering Residency: Toolkits for the 13 Core EPAs. 2014. [Online]. Available: https://www.aamc.org/media/20196/download

[16] R. Englander et al. "Toward Defining the Foundation of the MD Degree: Core Entrustable Professional Activities for Entering Residency," Journal of the Association of American Medical Colleges, vol. 91, no. 10, pp. 1352-1358,(2016). https://doi.org/10.1097/ACM.0000000000001204

[17] A. Sterkenburgm, P. Barach, C. Kalkman, M. Gielen, and C. O. Ten. "When do supervising physicians decide to entrust residents with unsupervised tasks?" Acad Med. ;85:1408–1417. 2010

[18] T. J. Kennedy, G. Regehr, G. R. Baker and L. Lingard. "Point-of-care assessment of medical trainee competence for independent clinical work," Acad Med. 83(10 suppl): S89–S92. 2008.

[19] K. Lomis, et al. "AAMC Core EPAs for Entering Residency Pilot Team. Implementing an Entrustable Professional Activities Framework in Undergraduate Medical Education: Early Lessons From the AAMC Core Entrustable Professional Activities for Entering Residency Pilot," Acad Med, vol. 92, no. 6, pp. 765-770, 2017. [Online]. Available: doi: 10.1097/ACM.0000000000001543.

[20] A. M. Garber, M. S. Ryan, S. A. Santen, and S. R. Goldberg. "Redefining the Acting Internship in the Era of Entrustment: One Institution's Approach to Reforming the Acting Internship. Med.Sci.Educ." 29, 583–591. 2019. [Online]. Available: https://doi.org/10.1007/s40670-019-00692-7

[21] B. Murphy. "3 ways the AMA is reshaping medical education," 2021. [Online]. Available: https://www.ama-assn.org/education/accelerating-change-medical-education/3-ways-ama-reshaping-medical-education

[22] T. C. Olle. "A primer on entrustable professional activities," 2017. [Online]. Available: https://scielo.isciii.es/pdf/fem/v20n3/2014-9832-fem-20-3-95a.pdf

[23] NIST. "Cybersecurity Workforce RFI," 2017. [Online]. Available: https://www.nist.gov/system/files/documents/2017/07/21/fairleigh_dickinson_university.pdf

[24] M. Prebil. Teach Cybersecurity with Apprenticeship Instead. New America. 2017. [Online]. Available: https://www.newamerica.org/education-policy/edcentral/teach-cyber-apprenticeship-instead/

[25] Whitehouse. "Executive Order 13870—America's Cybersecurity Workforce," 2019. [Online]. Available: https://www.govinfo.gov/content/pkg/DCPD-201900266/pdf/DCPD-201900266.pdf

[26] K. J. Knapp, C. Maurer, and M. Plachkinova. "Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance." Journal of Information Systems Education 28.2 . 2017: 101.

[27] National Initiatives for Cybersecurity Careers and Studies (NICCS). "NICE Framework Work Roles. Cyber Operator." 2020. [Online]. Available: https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework/workroles?name=Cyber+Operator&id=All

[28] Information-technology Promotion Agency (IPA). "iCD Pocket Handbook. 2017." [Online]. Available: https://www.ipa.go.jp/files/000061798.pdf

[29] National Initiatives for Cybersecurity Careers and Studies (NICCS). "NICE Framework Work Roles. Cyber Defense Analyst." 2020. [Online]. Available: https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework/workroles?name=Cyber+Defense+Analyst&id=All