A Critical Review of Cybersecurity Education in the United States

James Crabb
jamescrabb@wsu.edu
School of Electrical Engineering and Computer Science
Washington State University
Pullman, Washington, United States

Christopher Hundhausen
chris.hundhausen@oregonstate.edu
School of Electrical Engineering and Computer Science
Oregon State University
Corvallis, Oregon, United States

Assefaw Gebremedhin
assefaw.gebremedhin@wsu.edu
School of Electrical Engineering and Computer Science
Washington State University
Pullman, Washington, United States

ABSTRACT

This work examines the state-of-the-art of cybersecurity education in the United States by considering two sources of data. The first source consists of Programs of Study for cybersecurity programs at Centers of Academic Excellence in Cybersecurity designated by the National Security Agency. Statistics were aggregated from a sample of one hundred CAE-C institutions, trends and gaps are identified, and improvements are proposed. The second source is peer-reviewed research published in the field of cybersecurity education over the last decade. A review of this literature shows a strong focus on identifying instructional content and developing educational tools while simultaneously indicating a shortage of research into rigorous evaluation of the instructional approaches being used to teach cybersecurity. Our review of these two sources of data highlight two paths to improving cybersecurity education in the United States. First, institutions offering cybersecurity degrees could work more closely with groups such as NIST, ACM, and IEEE to ensure their curricula match the needs of industry and they are graduating work-ready cybersecurity specialists. While CAE-C designation provides certain requirements for the amount of cybersecurity content included in curricula, designated institutions vary widely in the types of programs they offer and how many cybersecurity-specific courses they provide. Second, cybersecurity education could benefit from an influx of ideas from educational psychology regarding instructional theories such as cognitive load theory.

CCS CONCEPTS

• **Social and professional topics** → **Computing education programs**; **Model curricula**; *Employment issues*; Computing organizations.

KEYWORDS

cybersecurity, education, curriculum, instructional design

ACM Reference Format:
James Crabb, Christopher Hundhausen, and Assefaw Gebremedhin. 2024. A Critical Review of Cybersecurity Education in the United States. In *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE 2024), March 20–23, 2024, Portland, OR, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3626252.3630757

SIGCSE 2024, March 20–23, 2024, Portland, OR, USA

ACM ISBN 979-8-4007-0423-9/24/03.
https://doi.org/10.1145/3626252.3630757

1 INTRODUCTION

Cybersecurity is commonly recognized as a critical field in modern society. Compromised data or network infrastructure can directly impact privacy, livelihood, and safety on an individual level, as well as have major consequences on a national or global level. Professionals in the cybersecurity field must be able to respond effectively to attacks carried out by adversaries with rapidly changing tactics. To minimize the chance of a successful attack, these professionals must be trained at the highest level possible, and must be able to adapt quickly to new threats. In order to ensure that the cybersecurity workforce in the United States is receiving the best training, we must periodically review how we are training our workforce, with a critical eye toward areas that need improvement.

To that end, the goal of this work is to perform a critical examination, identify deficiencies in the ways cybersecurity professionals in the United States are being educated and trained, and suggest remedies. One known problem in cybersecurity education is the *skill gap* between what college graduates are capable of and what industry employers expect of them. This is widely recognized as an important issue [9, 10, 26, 60]. Two significant efforts aimed at closing this gap are the Workforce Framework for Cybersecurity (NICE Framework) [53] and the Computing Curricula 2020 report (CC2020) [20]. These works represent two sides of the same coin: approaching the cybersecurity skill gap from the perspective of industry (NICE Framework) and that of academia (CC2020).

The NICE Framework defines a common language for communicating about work role requirements for a range of cybersecurity jobs, and the CC2020 establishes a similar system for describing and tracking competencies taught in computing courses and curricula. Whereas the CC2020 addresses the broader field of computing, the Cybersecurity Curricula 2017 (CSEC2017) [33] identifies important topics within the subdomain of cybersecurity and is referenced in the CC2020. Additionally, the National Security Agency (NSA) and Department of Homeland Security (DHS) lead an initiative to certify institutions of higher education in the U.S. as Centers of Academic Excellence in Cybersecurity (CAE-C) [48], requiring designated institutions to offer courses covering certain general computing and cybersecurity-related topics.

Section 2 of this paper analyzes public data gathered from CAE-C institutions in order to identify common traits and variability among these exemplar cybersecurity programs. Section 3 presents a systematic literature review of cybersecurity education research published over the last ten years. The goal is to identify current trends in cybersecurity instructional design as reflected by recent research on instructional content, tools, and methodologies (collectively, *pedagogies*) specific to cybersecurity. We expect this type of research to be impactful to the development of programs such as

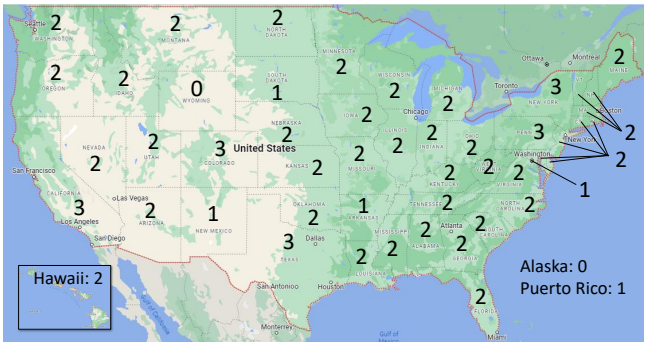

Figure 1: Number of sampled CAE-C institutions in each state/area. Background map credit: Google Maps.

those discussed in Section 2. Although sections 2 and 3 are diverse in their analytical approaches, together they provide a broader view of cybersecurity education trends. Section 4 presents conclusions.

2 CYBERSECURITY PROGRAMS AT CENTERS OF ACADEMIC EXCELLENCE IN CYBERSECURITY

Institutions holding a CAE-C designation have undergone a rigorous application process and been deemed exemplars in cybersecurity education and training by the NSA and DHS. To understand how cybersecurity is being taught at the highest level in the U.S., we analyze a sample of these institutions.

2.1 Methods

There are currently 377 institutions with one or more current CAE-C designations valid through at least 2023. These institutions are distributed throughout 48 states, the District of Columbia, and Puerto Rico [13]. To make this review manageable, we sampled a total of 100 institutions, with the goal of including two institutions from each state or region, so as to obtain a "nation-wide view" of CAE-C institutions (see Figure 1). We only included institutions with Cyber Defense (CD) or Cyber Operation (CO) designations because they address undergraduate programs, while the third designation, Research, strictly relates to graduate programs. Institutions were sampled randomly from within states when possible, but five states or regions had only one institution to include in our sample (Arkansas, District of Columbia, New Mexico, Puerto Rico and South Dakota) and two states had no CAE-C institutions (Alaska and Wyoming). Upon request, we are happy to provide a complete list of the 100 institutions sampled.

We needed to replace a small number of institutions because they lacked key information on their websites. In each case except Puerto Rico, it was possible to choose another institution from that same region, although not always randomly as in cases with only one other institution to choose from. To reach the target sample size of 100, additional institutions were chosen randomly from states having a large number of qualifying institutions (one each): California, Colorado, New York, Pennsylvania, and Texas.

We used information available on each sampled institution's website to ascertain the following: the number and type of cybersecurity programs offered; the total number of credits required by a program; the number of credits required by a program that could be attributed to a cybersecurity course; the college or school housing the program(s); the title of the program; whether the program's description mentions the NICE Framework, CSEC2017, CC2020, or the institution's CAE-C designation; whether the program's description includes a list of student learning outcomes; and whether the program's description includes a list of potential job titles graduates should be qualified for.

The cybersecurity programs in the sample could be classified as Bachelor's Degrees, concentrations or tracks within degrees other than cybersecurity, Associate Degrees, minors, and certificates. We counted required credit amounts for one "primary" program at each sampled institution, which was determined using the priority order listed in the previous sentence. Exact required credit amounts were provided for most programs, and required cybersecurity credits could be counted for most programs. A total of 15 samples did *not* display credit amounts, either total or by course, in a way that made it possible to count them. Required credits were considered to be "cybersecurity credits" if the course they were associated with met two criteria: The course must be required, and the title of the course must relate to one or more of the eight Knowledge Areas described in the CSEC2017 [33]. Although many courses with a broader focus may still discuss cybersecurity topics, the main focus of the course needed to clearly be cybersecurity.

We collected program titles for one primary program (described above) at each institution. Determining the college or school housing the program(s) was straightforward in about half of samples, but unclear in 46 samples, so it was not recorded in those cases.

We considered a program's description to mention the NICE Framework, CSEC2017, CC2020, student learning outcomes, or potential job titles if these were clearly referenced in text describing the program in question, or in the case of an institution's CAE-C designation, if it was clearly stated in a location that a visitor to the website interested in cybersecurity programs could be reasonably expected to visit.

2.2 Results

Of the 100 CAE-C designated institutions sampled, 50 offered Bachelor's Degrees, 35 offered certificates, 32 offered Associate Degrees, 16 offered minors, and 14 offered concentrations or tracks within a non-cybersecurity Bachelor's or Associate Degree. This is shown in Figure 2 (black bars) along with the total number of programs across all institutions (gray bars). Differences between the bars stem from institutions offering multiple programs of a given type. Of the Bachelor's Degree programs, including concentrations, 49 are Bachelor of Science, four are Bachelor of Applied Science, two are Bachelor of Art, and four don't specify which type they are. Figure 3 shows a box plot of the percentages of cybersecurity credits required for degree programs and concentrations, based on a sample of 75 institutions—one primary program at each institution. Box plots show the first and third quartiles in the box separated by the median and the "whiskers" show variation outside this range. The mean is marked by an × and circles (○) show outliers.

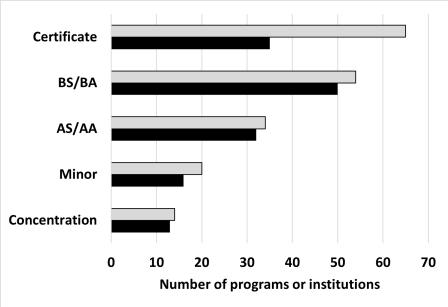

Figure 2: Number of programs offered by sampled CAE-C institutions. Gray bar displays total number of programs of each type. Black bar displays the number of institutions housing that type of program. Differences between gray and and black bars occur because single institutions can offer multiple programs of a given type.

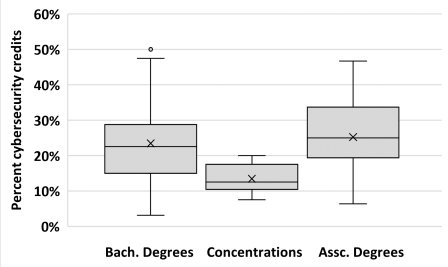

Figure 3: Percent of total required credits from cybersecurity courses.

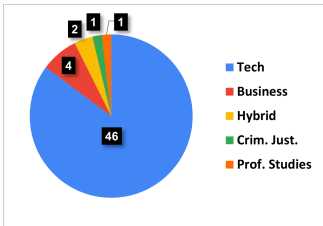

Figure 4: Number of programs housed by college/school.

Figure 4 classifies the 54 programs whose specific college, school, or department could be identified. "Tech" refers to Computer Science-, Technology-, or Engineering-type organizations (a college, school or department), "hybrid" refers to combined Business and Technology organizations, "Crim. Just." refers to a Department of Criminal Justice and Criminology, and "Prof. Studies" refers to a College of Professional Studies.

Across all 100 institutions, 46 advertise their CAE-C designation. Eight program descriptions reference the NICE Framework, two reference the CSEC2017, and none reference the CC2020. Twenty-six list learning outcomes and 20 list appropriate job titles in their program descriptions. Forty-one program titles are "Cybersecurity" or "Cyber Security", eight are "Computer Science - Cybersecurity", four are "Cybersecurity Engineering", three are "Cyber Operations", two are "Computer Science", two are "Information Assurance and Cybersecurity", two are "Information Technology", and the remaining 38 programs have unique names, most of which (27) include the word "cybersecurity."

2.3 Discussion

2.3.1 Application of the NICE Framework, CSEC2017 and CC2020. Requirements in the CAE-CD and CO program guides [6, 7] state that designated institutions are required to perform a "NICE Framework Crosswalk Alignment" in which they identify Categories from the NICE Framework that their program best supports. Although engagement with the NICE Framework is mandatory for CAE-C institutions, only 8% of program descriptions reference the NICE Framework and only 20% list targeted job types. Advertising a program's NICE Framework alignment is important as it can aid decision making for students and employers. Based on our results, the CSEC2017 and CC2020 do not seem to be widely adopted by CAE-C institutions, with only 2% referencing the CSEC2017, and none referencing the CC2020. While these may have broader adoption, it's impossible to tell from public information alone.

One way institutions could use these tools to address the skill gap discussed above is by using specifications in the NICE Framework *and* CSEC2017 along with methods laid out in the CC2020 for tracking and describing curricula, going beyond the NICE Framework Crosswalk Alignment required by the CAE-C program. This would allow comparison of curricula based on a common set of specifications to help both students and employers find ideal jobs and employees, which is one of the stated goals of the CC2020. Widespread adoption of tools such as the CSEC2017 and CC2020 by CAE-C institutions could have a broader positive impact across the country by encouraging other institutions to follow suit. The more institutions that adopt these tools, the more effective the tools themselves become as a means for communicating about cybersecurity curricula and ultimately helping to close the skill gap.

2.3.2 Variation across cybersecurity programs at CAE-C institutions. The majority of all CAE-C institutions hold CD designations (84%). Requirements for designation are laid out in the CAE-CD program guide [6]. An institution must provide a Program of Study (PoS) that covers certain Knowledge Units (KU) that fall into four categories: *Foundational* (IT Systems Components, Cybersecurity Foundations, Cybersecurity Principles), *Technical Core* (Basic Scripting and Programming, Basic Networking, Network Defense, Basic Cryptography, Operating Systems Concepts), *Non-Technical Core* (Cyber Threats, PLE (Policy, Legal Ethics and Compliance), Security Program Management, Security Risk Analysis, Cybersecurity Planning and Management), and *Optional* (the program guide [6] contains a full list in Appendix 1). *Foundational* KUs must all be covered by courses in the PoS. Programs have the choice of covering all *Technical Core* KUs *or* all *Non-Technical Core* KUs. There are 56 *Optional* KUs to choose from. Bachelor's programs must cover at least 14 of these, and Associate programs must cover at least three. A program may also use KUs from the *Core* group it does not cover as *Optional* KUs.

From the KUs' titles, it is clear that some are general computer science topics and others are cybersecurity-specific topics. It is possible for a program to cover the *Foundational* KUs, *Technical Core* KUs and 14 general computer science topics, resulting in only four out of 22 (Bachelor's) or 11 (Associate) KUs in the program having a cybersecurity focus (18.2% or 36.4%, respectively). Alternatively, a program covering the *Foundational* KUs, *Non-Technical Core* KUs and 14 (or 3) cybersecurity-specific *Optional* KUs would have 20

of 21 (95.2%) or 10 of 11 (91%) cybersecurity KUs. This affords designated institutions a great deal of flexibility as to the number of cybersecurity-specific courses included in their programs and is reflected in the wide range of cybersecurity course credits included in Bachelor's and Associate Degree programs.

Although this variability in CAE-CD programs may appear to be a barrier to providing a national standard for cybersecurity education programs, it does allow a broader range of institutions to participate in the CAE-C program and offer a more diverse array of cybersecurity programs than would be possible under more stringent requirements. The key to benefiting from this diversity is clear and accurate communication regarding the strengths of individual programs so that students and employers can identify the best programs for them.

2.3.3 ABET requirements for cybersecurity degrees. Institutions aspiring to design a modern Bachelor of Science in Cybersecurity degree program that meets CAE-C designation requirements would simultaneously need to consider ABET requirements for such a degree. Accreditation is one of the CAE-C requirements for an institution to be designated, and in the computing domain, ABET is a well-known accrediting agency. ABET cybersecurity curriculum requirements specify topics, some of which align closely with CAE-C KUs, but do not prescribe specific courses. Fundamental topics are: *Data-*, *Software-*, *Component-*, *Connection-*, *System-*, *Human-*, *Organizational-* and *Societal Security*. Cross-cutting concepts are also required: *confidentiality*, *integrity*, *availability*, *risk*, *adversarial thinking* and *systems thinking*. Institutions must include courses covering these topics as well as advanced topics that extend the fundamental topics and provide program depth for a total of 45 semester credits. Additionally, these programs must include six semester credits of math, covering discrete math and statistics at a minimum [1].

One creative way in which these requirements can be met while still fitting into a typical four-year, 120-credit program is to design it as a "two-staged" program, where the the first two years are devoted to foundational computer science and mathematics topics, very similar to a typical BS in Computer Science program, and the last two years are heavy on cyber topics. Washington State University has successfully adopted this strategy to design its BS in Cybersecurity degree [69]. A potential concern with this approach may be that students are not introduced to cybersecurity topics until their junior or second semester of their sophomore year. However, this delay can be countered by exposing new students to contemporary issues and experiential learning in cybersecurity outside of the classroom through formats such as seminars, workshops and mentored research as is done by the VICEROY CySER program at WSU [17].

2.3.4 Comparison of the NICE Framework, CSEC2017, and CAE-C. Bloom's Revised Taxonomy [5] defines six cognitive levels involving the use of knowledge. From lowest to highest, they are *Remember*, *Understand*, *Apply*, *Analyze*, *Evaluate*, and *Create*. The NICE Framework, CSEC2017 and CC2020 all cite Bloom's Revised Taxonomy, and the CC2020 further maps Bloom's levels to skill level when performing tasks. By mapping TDs (NICE Framework) and learning outcomes (CSEC2017 and CAE-C) to Bloom's levels, we can compare the general level of expertise expected by these different bodies. Figure 5 shows the results of such a mapping performed using all 269 learning outcomes from both the CAE-CD and CO KU lists (available in the CAE Documents Library [47]), all 140 learning outcomes listed in the CSEC2017, and a sample of 270 TDs (out of a total 1,006) from the NICE Framework.

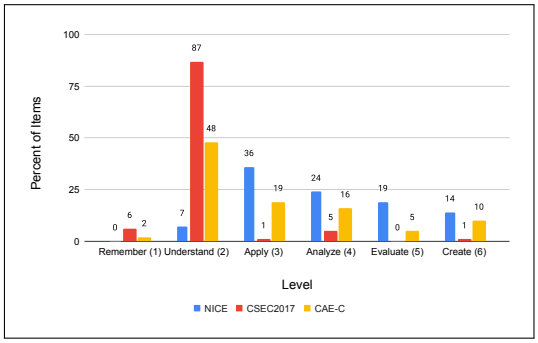

Figure 5: Percent of TDs/LOs mapped to Bloom's level. Each group of 3 bars from left to right are NICE Framework TDs, CSEC2017 LOs and CAE-C LOs.

A stark difference can be seen between the Bloom's levels of the CSEC2017 learning outcomes, the vast majority of which fall at the *Understand* level, and the NICE Framework TDs, which are distributed across the upper four levels: *Apply*, *Analyze*, *Evaluate*, and *Create*. The implication is that the NICE Framework, which represents industry needs, generally expects a higher level of expertise from cybersecurity professionals than the CSEC2017 is recommending students to achieve. This highlights one aspect of the cybersecurity skill gap: a difference in the expectations of industry and academia.

3 LITERATURE REVIEW OF CYBERSECURITY EDUCATION RESEARCH

Here we present our review of contemporary research on cybersecurity education to analyze the foundational work being done which has direct applications to how the programs discussed in the previous section are being designed and taught. Indeed, both ABET and the CAE-C program require institutions to have a Continuous Improvement Plan whereby programs are evaluated and weaknesses can be addressed. Such improvement is supported by research that tests our current assumptions about how best to teach cybersecurity.

3.1 Methods

Our review is based on sources available in the ACM Digital Library and IEEE Xplore databases. It includes "research articles" (ACM) and "journal papers" and "conference papers" (IEEE) published within the last 10 years (2014-2023) using the search term "cyber* AND educat*". Papers were sorted by relevance and then a total of 80 from IEEE Xplore and 51 from ACM Digital Library were checked against inclusion/exclusion criteria before identifying 25 publications from each database that met these criteria. Papers discussing higher education were included, whereas papers solely discussing

K-12 education or non-expert training were excluded. Included papers were required to have a focus on instructional content, tools, or methods. We also recorded whether or not they reported any empirical comparisons between different content, tools, or methods.

Content refers to the topics being taught in a course. For example, the NICE Framework, CSEC2017 and CAE-CD KU requirements deal with instructional content because they identify specific skills and learning outcomes. Tools refer to infrastructure applied within a course in order to facilitate instruction such as reading materials, lecture materials, hardware and software. Tools convey content to learners. Examples of tools involving hardware and software include capture-the-flag events and cyber ranges. Instructional methods are the teaching strategies behind how tools are employed. For example, an instructor may give an assigned reading (the tool) on some topic (the content) to a group of students and ask them to generate a summary of it individually or as a group (two different methods).

3.2 Results

A total of 50 papers were included in this review. Of these, 21 focused on instructional tools, 19 on instructional content, and 10 on instruction methods. The references for these papers are listed in Table 1. No papers from the Content category, two papers from the Tools category [18, 49] and six papers from the Methods category [14, 19, 32, 40, 57, 68] reported results of empirical studies comparing two or more types of content, tools or methods.

Table 1: Focus of research in cybersecurity education

Focus	Count	References
Tools	21	[2, 16, 18, 21, 27, 36–39, 41, 42, 45, 46, 49, 52, 59, 62, 64, 65, 67, 70]
Content	19	[3, 8, 11, 12, 24, 25, 29–31, 34, 35, 44, 50, 51, 54–56, 58, 61]
Methods	10	[4, 14, 19, 22, 23, 28, 32, 40, 57, 68]

3.3 Discussion

Of the 50 papers included in this review, 42% reported on instructional tools, 38% on instructional content, and 20% on instructional methods. Across all papers, just 16% included results of empirical studies comparing two or more tools or methods. Based on this review, there appears to be a stronger emphasis on developing new instructional tools and identifying important instructional content than on developing or improving instructional methods for teaching cybersecurity. This concurs with a review by Švábenský et al. [66], which concluded that cybersecurity education research could benefit from additional rigor in conducting evaluations and reporting methods.

The cybersecurity education community would be well served if more researchers included rigorous evaluations of the efficacy of content, tools and methods. Such evaluations are common in the field of educational psychology, which has developed concepts and theories that could be applied to cybersecurity education, such as cognitive load theory [63], the ICAP framework [15], and intrinsic motivation theory [43]. Such theories could be applied and tested in cybersecurity classrooms to help improve instructional design. Some of the papers included in this review reference theories or frameworks from educational psychology [19, 23, 32], so they are not unheard of within the context of cybersecurity education—just not widely applied.

4 CONCLUSIONS

The CAE-C program currently includes 377 institutions that offer programs in cybersecurity that adhere to the CAE-C's requirements for educational content and quality. These institutions and their programs represent a benchmark that can be used to compare cybersecurity programs across the United States. As such, it is important to understand key traits of these programs. To that end, we have presented a review of 100 CAE-C institutions representing almost the entire geography of the United States.

The most common type of program at these institutions were certificates, with a total of 65 being offered at 35 different locations. The next most common are four year degrees (mainly Bachelor of Science) specifically in cybersecurity with a total of 54 being offered across 50 institutions. The vast majority of these programs are housed in colleges, schools or departments dedicated to Technology, Engineering, and/or Computer Science. Although there exists diversity in program names, the most common title is "Cybersecurity." The number of cybersecurity courses included in each program varies widely between institutions, because the requirements of the CAE-C program are flexible in terms of instructional content. Although this reduces standardization across CAE-C institutions, it may encourage a greater diversity of programs that meet the needs of different industry sectors. Clear communication of program content and target job types is key.

Projects like the NICE Framework, CSEC2017 and CC2020 aim to address the current skill gap between cybersecurity graduates and professionals. This is critical if the United States is to maintain a competitive edge against adversaries in the cyber domain. Our comparison of the NICE Framework, CSEC2017 and CAE-C using Bloom's Revised Taxonomy to classify Task Descriptions and learning outcomes shows a disparity between the expected skill level of cybersecurity professionals and the skill level achieved by cybersecurity graduates. Narrowing this gap by raising academic expectations is one way to help close the United States' cybersecurity skill gap.

Another path to closing this skill gap is to improve instructional design for cybersecurity education. The literature review we conducted could be extended to include additional databases and consider a larger number of publications. Our intent was not to be exhaustive, but rather to identify certain broad trends occurring in research into cybersecurity instructional design because it has a direct impact on how cybersecurity courses and curricula are designed and improved moving forward. Currently, such research is dominated by instructional tools and content, with a low proportion of research focused on instructional methods or empirical evaluation of the efficacy of instructional tools, content, and methods. Concepts and tools from educational psychology do not seem to be well adopted within cybersecurity education research. Methodical improvement of instructional design for cybersecurity requires rigorous testing of pedagogies, which would be facilitated by a broader application of educational psychology to cybersecurity.

ACKNOWLEDGMENTS

This work is supported in part by funding for the VICEROY Northwest Institute for Cybersecurity Education and Research (CySER) provided by The Office of the Undersecretary of Defense for Research and Engineering, in collaboration with the Air Force Research Laboratory and Griffiss Institute.

REFERENCES

[1] ABET. 2023. Criteria for Accrediting Computing Programs, 2023-2024. https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2023-2024/. Accessed: 2023-10-23.

[2] Uttam Adhikari, Thomas Morris, and Shengyi Pan. 2017. WAMS Cyber-Physical Test Bed for Power System, Cybersecurity Study, and Data Mining. *IEEE Transactions on Smart Grid* 8, 6 (2017), 2744–2753. https://doi.org/10.1109/TSG.2016.2537210

[3] Norita Ahmad, Phillip A. Laplante, Joanna F. DeFranco, and Mohamad Kassab. 2022. A Cybersecurity Educated Community. *IEEE Transactions on Emerging Topics in Computing* 10, 3 (2022), 1456–1463. https://doi.org/10.1109/TETC.2021.3093444

[4] Isabel Borges Alvarez, Nuno S. Alves Silva, and Luisa Sampaio Correia. 2016. Cyber Education: Towards a Pedagogical and Heuristic Learning. *SIGCAS Comput. Soc.* 45, 3 (jan 2016), 185–192. https://doi.org/10.1145/2874239.2874266

[5] L.W. Anderson, D.R. Krathwohl, P.W. Airasian, K.A. Cruikshank, R.E. Mayer, P.R. Pintrich, J. Raths, and M.C. Wittrock. 2001. *A taxonomy for learning, teaching, and assessing: A revision of Bloom's Taxonomy of Educational Objectives.* Longman, New York.

[6] Application Process and Adjudication Rubric, Cyber Defense Working Group. 2022. *National Centers of Academic Excellence in Cybersecurity CAE 2022, Designation requirements and application process for CAE-Cyber Defense.* NCyTE Center at Whatcom Community College, Bellingham, WA.

[7] Application Process and Adjudication Rubric, Cyber Defense Working Group. 2022. *National Centers of Academic Excellence in Cybersecurity CAE 2022, Designation requirements and application process for CAE-Cyber Operations.* NCyTE Center at Whatcom Community College, Bellingham, WA.

[8] Miriam E. Armstrong, Keith S. Jones, Akbar Siami Namin, and David C. Newton. 2020. Knowledge, Skills, and Abilities for Specialized Curricula in Cyber Defense: Results from Interviews with Cyber Professionals. *ACM Trans. Comput. Educ.* 20, 4, Article 29 (nov 2020), 25 pages. https://doi.org/10.1145/3421254

[9] Sam Attwood and Ashley Williams. 2023. Exploring the UK Cyber Skills Gap through a Mapping of Active Job Listings to the Cyber Security Body of Knowledge (CyBOK). In *Proceedings of the 27th International Conference on Evaluation and Assessment in Software Engineering* (Oulu, Finland) *(EASE '23)*. Association for Computing Machinery, New York, NY, USA, 273–278. https://doi.org/10.1145/3593434.3593459

[10] Louise Axon, Katherine Fletcher, Arianna Schuler Scott, Marcel Stolz, Robert Hannigan, Ali El Kaafarani, Michael Goldsmith, and Sadie Creese. 2022. Emerging Cybersecurity Capability Gaps in the Industrial Internet of Things: Overview and Research Agenda. *Digital Threats* 3, 4, Article 34 (dec 2022), 27 pages. https://doi.org/10.1145/3503920

[11] Sagar Behere and Martin Törngren. 2017. Educating Embedded Systems Hackers: A Practitioner's Perspective. *SIGBED Rev.* 14, 1 (jan 2017), 8–15. https://doi.org/10.1145/3036686.3036687

[12] Bruce D. Caulkins, Karla Badillo-Urquiola, Patricia Bockelman, and Rebecca Leis. 2016. Cyber workforce development using a behavioral cybersecurity paradigm. In *2016 International Conference on Cyber Conflict (CyCon U.S.)*. 1–6. https://doi.org/10.1109/CYCONUS.2016.7836614

[13] Centers of Academic Excellence in Cybersecurity Community. 2023. CAE Institution Map. https://www.caecommunity.org/cae-map. Accessed: 2023-08-18.

[14] Ankur Chattopadhyay, Mohammad Q. Azhar, Thomas Everson, and Robert Ruska Jr. 2020. Integrated Cybersecurity Plus Robotics Lesson Using NAO. In *Proceedings of the 21st Annual Conference on Information Technology Education* (Virtual Event, USA) *(SIGITE '20)*. Association for Computing Machinery, New York, NY, USA, 397–402. https://doi.org/10.1145/3368308.3415418

[15] Michelene TH Chi and Ruth Wylie. 2014. The ICAP framework: Linking cognitive engagement to active learning outcomes. *Educational psychologist* 49, 4 (2014), 219–243.

[16] Te-Shun Chou and John Jones. 2018. Developing and Evaluating an Experimental Learning Environment for Cyber Security Education. In *Proceedings of the 19th Annual SIG Conference on Information Technology Education* (Fort Lauderdale, Florida, USA) *(SIGITE '18)*. Association for Computing Machinery, New York, NY, USA, 92–97. https://doi.org/10.1145/3241815.3241855

[17] CySER. 2023. VICEROY Northwest Institute for Cybersecurity Education and Research. https://cyser.wsu.edu/. Accessed: 2023-10-23.

[18] Pranita Deshpande and Irfan Ahmed. 2019. Topological Scoring of Concept Maps for Cybersecurity Education. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education* (Minneapolis, MN, USA) *(SIGCSE '19)*. Association for Computing Machinery, New York, NY, USA, 731–737. https://doi.org/10.1145/3287324.3287495

[19] Pranita Deshpande, Cynthia B. Lee, and Irfan Ahmed. 2019. Evaluation of Peer Instruction for Cybersecurity Education. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education* (Minneapolis, MN, USA) *(SIGCSE '19)*. Association for Computing Machinery, New York, NY, USA, 720–725. https://doi.org/10.1145/3287324.3287403

[20] CC2020 Task Force. 2020. *Computing Curricula 2020: Paradigms for Global Computing Education.* Association for Computing Machinery, New York, NY, USA.

[21] Maximilian Frank, Maria Leitner, and Timea Pahi. 2017. Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education. In *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*. 38–46. https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2017.23

[22] Paul J. Frontera and Erick J. Rodríguez-Seda. 2021. Network Attacks on Cyber–Physical Systems Project-Based Learning Activity. *IEEE Transactions on Education* 64, 2 (2021), 110–116. https://doi.org/10.1109/TE.2020.3014268

[23] Thoshitha Gamage and Tim York. 2021. Reflections of a Hardware-Software Co-Instructional Approach to Cybersecurity Education. In *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education* (Virtual Event, USA) *(SIGCSE '21)*. Association for Computing Machinery, New York, NY, USA, 1219–1225. https://doi.org/10.1145/3408877.3432473

[24] Edward J. Glantz, Michael R. Bartolacci, Mahdi Nasereddin, and David Joseph Fusco. 2020. Cross-Boundary Cyber Education Design. In *Proceedings of the 21st Annual Conference on Information Technology Education* (Virtual Event, USA) *(SIGITE '20)*. Association for Computing Machinery, New York, NY, USA, 336–341. https://doi.org/10.1145/3368308.3415374

[25] Edward J. Glantz, Michael R. Bartolacci, Mahdi Nasereddin, David J. Fusco, Joanne C. Peca, and Devin Kachmar. 2021. Wireless Cybersecurity Education: A Focus on Curriculum. In *2021 Wireless Telecommunications Symposium (WTS)*. 1–5. https://doi.org/10.1109/WTS51064.2021.9433709

[26] Francois Goupil, Pavel Laskov, Irdin Pekaric, Michael Felderer, Alexander Dürr, and Frederic Thiesse. 2022. Towards Understanding the Skill Gap in Cybersecurity. In *Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 1* (Dublin, Ireland) *(ITiCSE '22)*. Association for Computing Machinery, New York, NY, USA, 477–483. https://doi.org/10.1145/3502718.3524807

[27] Kendra Graham, James Anderson, Conrad Rife, Bryce Heitmeyer, Pranav R. Patel, Scott Nykl, Alan C. Lin, and Laurence D. Merkle. 2020. Cyberspace Odyssey: A Competitive Team-Oriented Serious Game in Computer Networking. *IEEE Transactions on Learning Technologies* 13, 3 (2020), 502–515. https://doi.org/10.1109/TLT.2020.3008607

[28] Said Saidakhrarovich Gulyamov, Andrey Aleksandrovich Rodionov, Islambek Rustambekovich Rustambekov, and Akhtam Nusrotilloyevich Yakubov. 2023. The Growing Significance of Cyber Law Professionals in Higher Education: Effective Learning Strategies and Innovative Approaches. In *2023 3rd International Conference on Technology Enhanced Learning in Higher Education (TELE)*. 117–119. https://doi.org/10.1109/TELE58910.2023.10184186

[29] Jan Hajny, Sara Ricci, Edmundas Piesarskas, Olivier Levillain, Letterio Galletta, and Rocco De Nicola. 2021. Framework, Tools and Good Practices for Cybersecurity Curricula. *IEEE Access* 9 (2021), 94723–94747. https://doi.org/10.1109/ACCESS.2021.3093952

[30] Jan Hajny, Sara Ricci, Edmundas Piesarskas, and Marek Sikora. 2021. Cybersecurity Curricula Designer. In *Proceedings of the 16th International Conference on Availability, Reliability and Security* (Vienna, Austria) *(ARES 21)*. Association for Computing Machinery, New York, NY, USA, Article 144, 7 pages. https://doi.org/10.1145/3465481.3469183

[31] Seth T. Hamman, Kenneth M. Hopkinson, Ruth L. Markham, Andrew M. Chaplik, and Gabrielle E. Metzler. 2017. Teaching Game Theory to Improve Adversarial Thinking in Cybersecurity Students. *IEEE Transactions on Education* 60, 3 (2017), 205–211. https://doi.org/10.1109/TE.2016.2636125

[32] Jason Hussey and Jacob Shaha. 2017. Educational Approach to Cyber Foundations in an Undergraduate Core Program. In *Proceedings of the 18th Annual Conference on Information Technology Education* (Rochester, New York, USA) *(SIGITE '17)*. Association for Computing Machinery, New York, NY, USA, 21–26. https://doi.org/10.1145/3125659.3125691

[33] 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.

[34] Hwee-Joo Kam and Pairin Katerattanakul. 2014. Diversifying cybersecurity education: A non-technical approach to technical studies. In *2014 IEEE Frontiers in Education Conference (FIE) Proceedings*. 1–4. https://doi.org/10.1109/FIE.2014.7044197

[35] Gary C. Kessler and James D. Ramsay. 2014. A Proposed Curriculum in Cybersecurity Education Targeting Homeland Security Students. In *2014 47th Hawaii International Conference on System Sciences*. 4932–4937. https://doi.org/10.1109/HICSS.2014.605

[36] Eunyoung Kim and Razvan Beuran. 2018. On Designing a Cybersecurity Educational Program for Higher Education. In *Proceedings of the 10th International Conference on Education Technology and Computers* (Tokyo, Japan) *(ICETC '18)*. Association for Computing Machinery, New York, NY, USA, 195–200. https://doi.org/10.1145/3290511.3290524

[37] Donghwan Lee, Donghwa Kim, Changwon Lee, Myung Kil Ahn, and Wonjun Lee. 2022. ICSTASY: An Integrated Cybersecurity Training System for Military Personnel. *IEEE Access* 10 (2022), 62232–62246. https://doi.org/10.1109/ACCESS.2022.3182383

[38] Phil Legg, Thomas Higgs, Pennie Spruhan, Jonathan White, and Ian Johnson. 2021. "Hacking an IoT Home": New opportunities for cyber security education combining remote learning with cyber-physical systems. In *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. 1–4. https://doi.org/10.1109/CyberSA52016.2021.9478251

[39] Kees Leune and Salvatore J. Petrilli. 2017. Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. In *Proceedings of the 18th Annual Conference on Information Technology Education* (Rochester, New York, USA) *(SIGITE '17)*. Association for Computing Machinery, New York, NY, USA, 47–52. https://doi.org/10.1145/3125659.3125686

[40] Qiang Liu, Wentao Zhao, Ruijin Wang, and Jiangyong Shi. 2021. A Competence-Based Three-Layer Cybersecurity Education Framework and Its Application. In *Proceedings of the ACM Turing Award Celebration Conference - China* (Hefei, China) *(ACM TURC '21)*. Association for Computing Machinery, New York, NY, USA, 54–60. https://doi.org/10.1145/3472634.3472649

[41] Xuan Low, DeQuan Yang, and DengPan Yang. 2022. Design and Implementation of Industrial Control Cyber Range System. In *2022 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*. 166–170. https://doi.org/10.1109/CyberC55534.2022.00034

[42] Marcin Lukowiak, Stanisław Radziszowski, James Vallino, and Christopher Wood. 2014. Cybersecurity Education: Bridging the Gap Between Hardware and Software Domains. *ACM Trans. Comput. Educ.* 14, 1, Article 2 (mar 2014), 20 pages. https://doi.org/10.1145/2538029

[43] Thomas W. Malone. 1981. Toward a theory of intrinsically motivating instruction. *Cognitive Science* 5, 4 (1981), 333–369. https://doi.org/10.1016/S0364-0213(81)80017-1

[44] Daniel Manson and Ronald Pike. 2014. The Case for Depth in Cybersecurity Education. *ACM Inroads* 5, 1 (mar 2014), 47–52. https://doi.org/10.1145/2568195.2568212

[45] Vimalnath N. Mathoosoothenen, Jakanath S. Sundaram, Ram A. Palanichamy, and Sarfraz N. Brohi. 2017. An Integrated Real-Time Simulated Ethical Hacking Toolkit with Interactive Gamification Capabilities and Cyber Security Educational Platform. In *Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence* (Jakarta, Indonesia) *(CSAI '17)*. Association for Computing Machinery, New York, NY, USA, 199–202. https://doi.org/10.1145/3168390.3168397

[46] Xenia Mountrouidou, Xiangyang Li, and Quinn Burke. 2018. Cybersecurity in Liberal Arts General Education Curriculum. In *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* (Larnaca, Cyprus) *(ITiCSE 2018)*. Association for Computing Machinery, New York, NY, USA, 182–187. https://doi.org/10.1145/3197091.3197110

[47] National Centers of Academic Excellence in Cybersecurity. 2023. CAE Document Library. https://public.cyber.mil/ncae-c/documents-library/. Accessed: 2023-08-18.

[48] National Security Agency. 2023. National Centers of Academic Excellence in Cybersecurity. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/. Accessed: 2023-08-18.

[49] Sang Keun Oh, Nathaniel Stickney, Daniel Hawthorne, and Suzanne J. Matthews. 2020. Teaching Web-Attacks on a Raspberry Pi Cyber Range. In *Proceedings of the 21st Annual Conference on Information Technology Education* (Virtual Event, USA) *(SIGITE '20)*. Association for Computing Machinery, New York, NY, USA, 324–329. https://doi.org/10.1145/3368308.3415364

[50] Geet Parekh, David DeLatte, Geoffrey L. Herman, Linda Oliva, Dhananjay Phatak, Travis Scheponik, and Alan T. Sherman. 2018. Identifying Core Concepts of Cybersecurity: Results of Two Delphi Processes. *IEEE Transactions on Education* 61, 1 (2018), 11–20. https://doi.org/10.1109/TE.2017.2715174

[51] Allen Parrish, John Impagliazzo, Rajendra K. Raj, Henrique Santos, Muhammad Rizwan Asghar, Audun Jøsang, Teresa Pereira, and Eliana Stavrou. 2018. Global Perspectives on Cybersecurity Education for 2030: A Case for a Meta-Discipline. In *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* (Larnaca, Cyprus) *(ITiCSE 2018 Companion)*. Association for Computing Machinery, New York, NY, USA, 36–54. https://doi.org/10.1145/3293881.3295778

[52] Animesh Pattanayak, Daniel M. Best, Daniel Sanner, and Jessica Smith. 2018. Advancing Cybersecurity Education: Pink Elephant Unicorn. In *Proceedings of the Fifth Cybersecurity Symposium* (Coeur d' Alene, Idaho) *(CyberSec '18)*. Association for Computing Machinery, New York, NY, USA, Article 3, 7 pages. https://doi.org/10.1145/3212687.3212862

[53] Rodney Petersen, Danielle Santos, Karen Wetzel, Matthew Smith, Greg Witte, et al. 2020. Workforce framework for cybersecurity (NICE framework). *Special Publication (NIST SP) - 800-181 Rev. 1* (2020).

[54] Jyri Rajamäki. 2018. Industry-university collaboration on IoT cyber security education: Academic course: "Resilience of Internet of Things and cyber-physical systems". In *2018 IEEE Global Engineering Education Conference (EDUCON)*. 1969–1977. https://doi.org/10.1109/EDUCON.2018.8363477

[55] Nageswaree Kodai Ramsoonder, Selvamanee Kinnoo, Anna J Griffin, Craig Valli, and Nicola F. Johnson. 2020. Optimizing Cyber Security Education: Implementation of Bloom's Taxonomy for future Cyber Security workforce. In *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*. 93–98. https://doi.org/10.1109/CSCI51800.2020.00023

[56] Jessica M. Richards and Joseph J. Ekstrom. 2015. The Cyber Education Project and IT IAS Curriculum. In *Proceedings of the 16th Annual Conference on Information Technology Education* (Chicago, Illinois, USA) *(SIGITE '15)*. Association for Computing Machinery, New York, NY, USA, 173–178. https://doi.org/10.1145/2808006.2808035

[57] S. Ros, S. González, A. Robles, LL. Tobarra, A. Caminero, and Jesus Cano. 2020. Analyzing Students' Self-Perception of Success and Learning Effectiveness Using Gamification in an Online Cybersecurity Course. *IEEE Access* 8 (2020), 97718–97728. https://doi.org/10.1109/ACCESS.2020.2996361

[58] Karo Saharinen, Jaakko Backlund, and Jarmo Nevala. 2021. Assessing Cyber Security Education through NICE Cybersecurity Workforce Framework. In *Proceedings of the 12th International Conference on Education Technology and Computers* (London, United Kingdom) *(ICETC '20)*. Association for Computing Machinery, New York, NY, USA, 172–176. https://doi.org/10.1145/3436756.3437041

[59] Khaled Salah, Mohammad Hammoud, and Sherali Zeadally. 2015. Teaching Cybersecurity Using the Cloud. *IEEE Transactions on Learning Technologies* 8, 4 (2015), 383–392. https://doi.org/10.1109/TLT.2015.2424692

[60] Björn Siemers, Shadi Attarha, Jirapa Kamsamrong, Michael Brand, Maria Valliou, Ruta Pirta-Dreimane, Janis Grabis, Nadezhda Kunicina, Mike Mekkanen, Tero Vartiainen, and Sebastian Lehnhoff. 2021. Modern Trends and Skill Gaps of Cyber Security in Smart Grid : Invited Paper. In *IEEE EUROCON 2021 - 19th International Conference on Smart Technologies*. 565–570. https://doi.org/10.1109/EUROCON52738.2021.9535632

[61] Edward Sobiesk, Jean Blair, Gregory Conti, Michael Lanham, and Howard Taylor. 2015. Cyber Education: A Multi-Level, Multi-Discipline Approach. In *Proceedings of the 16th Annual Conference on Information Technology Education* (Chicago, Illinois, USA) *(SIGITE '15)*. Association for Computing Machinery, New York, NY, USA, 43–47. https://doi.org/10.1145/2808006.2808038

[62] Anurag K. Srivastava, Adam L. Hahn, Olusola O. Adesope, Carl H. Hauser, and David E. Bakken. 2017. Experience With a Multidisciplinary, Team-Taught Smart Grid Cyber Infrastructure Course. *IEEE Transactions on Power Systems* 32, 3 (2017), 2267–2275. https://doi.org/10.1109/TPWRS.2016.2611588

[63] John Sweller, Paul Ayres, and Slava Kalyuga. 2011. *Cognitive load theory* (1 ed.). Explorations in the learning sciences, instructional systems and performance technologies, Vol. 1. Springer, New York, NY.

[64] Eniye Tebekaemi and Martin Zhao. 2022. Cyber-Softbook: A Platform for Collaborative Content Development and Delivery for Cybersecurity Education. In *2022 IEEE Global Engineering Education Conference (EDUCON)*. 320–327. https://doi.org/10.1109/EDUCON52537.2022.9766639

[65] David H. Tobey, Portia Pusey, and Diana L. Burley. 2014. Engaging Learners in Cybersecurity Careers: Lessons from the Launch of the National Cyber League. *ACM Inroads* 5, 1 (mar 2014), 53–56. https://doi.org/10.1145/2568195.2568213

[66] Valdemar Švábenský, Jan Vykopal, and Pavel Čeleda. 2020. What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (Portland, OR, USA) *(SIGCSE '20)*. Association for Computing Machinery, New York, NY, USA, 2–8. https://doi.org/10.1145/3328778.3366816

[67] Le Wang, Zhihong Tian, Zhaoquan Gu, and Hui Lu. 2019. Crowdsourcing Approach for Developing Hands-On Experiments in Cybersecurity Education. *IEEE Access* 7 (2019), 169066–169072. https://doi.org/10.1109/ACCESS.2019.2952585

[68] Michael D. Workman, J. Anthony Luévanos, and Bin Mai. 2022. A Study of Cybersecurity Education Using a Present-Test-Practice-Assess Model. *IEEE Transactions on Education* 65, 1 (2022), 40–45. https://doi.org/10.1109/TE.2021.3086025

[69] WSU. 2023. The Washington State University Pullman Catalog - Cybersecurity. https://catalog.wsu.edu/Pullman/Academics/DegreeProgram/10631. Accessed: 2023-10-23.

[70] Jing Xie, Juan Carlos Bedoya, Chen-Ching Liu, Adam Hahn, Kudrat Jot Kaur, and Rajveer Singh. 2018. New Educational Modules Using a Cyber-Distribution System Testbed. *IEEE Transactions on Power Systems* 33, 5 (2018), 5759–5769. https://doi.org/10.1109/TPWRS.2018.2821178