A Critical Review of Cybersecurity Education in the United States

James Crabb  
James Crabb@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.

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 exemplary 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
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.
A Critical Review of Cybersecurity Education in the United States

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

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-C 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 benefitting 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 ABET-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.

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

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

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.