Knowledge, Skills, and Abilities for Specialized Curricula in Cyber Defense: Results from Interviews with Cyber Professionals

MIRIAM E. ARMSTRONG, KEITH S. JONES, and AKBAR SIAMI NAMIN,
Texas Tech University
DAVID C. NEWTON, Federal Aviation Administration & Texas Tech University

More specialized cybersecurity education programs are needed to address workforce needs, but it is unclear which knowledge, skills, and abilities (KSAs) fulfil industry needs. We interviewed 48 professionals within four cyber defense specialty areas: (1) Cyber Network Defense Analysis, (2) Cyber Network Defense Infrastructure Support, (3) Incident Response, and (4) Vulnerability Assessment and Management. The professionals rated a number of specialized KSAs along two dimensions: how important the KSA was to their job and how difficult the KSA was to learn. Overall, communication and other non-technical skills were rated as being very important for all cyber defense jobs. Findings indicated that, for some specialty areas, technical knowledge and skills vary considerably between jobs and so the ability to teach oneself is more valuable than proficiency in any one KSA. Findings may be used to inform the development of general cybersecurity curricula, as well as curricula that focus on Cyber Network Defense Analysis, Cyber Network Defense Infrastructure Support, or Vulnerability Assessment and Management.

CCS Concepts: • **Security and privacy** • **Social and professional topics** → **Computing education programs**; Employment issues;

Additional Key Words and Phrases: Cyber-defense, cybersecurity education, curricula development, NICE cybersecurity workforce framework

ACM Reference format:
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 (November 2020), 25 pages.
https://doi.org/10.1145/3421254

This research was supported by the National Science Foundation under the following award numbers: DGE 1516636, DGE 1723765, and 1564293.
Authors' addresses: M. E. Armstrong, K. S. Jones, and A. S. Namin, Texas Tech University, 2500 Broadway, Lubbock, TX 79409; emails: miriam.armstrong@ttu.edu, keith.s.jones@ttu.edu, akbar.namin@ttu.edu; D. C. Newton, Federal Aviation Administration & Texas Tech University, 6425 Denning Ave, Oklahoma City, OK 73169; email: david.newton@ttu.edu.

1946-6226/2020/11-ART29 $15.00
https://doi.org/10.1145/3421254

1 INTRODUCTION

Cyber defense is critical for modern economic and national security. Unfortunately, there is a global shortage of qualified cybersecurity professionals [20, 36, 48].

Lack of professionals who can protect and defend organizations from cyber attack leaves both public and private institutions and organizations vulnerable. Recently in the United States, the state of Colorado and city of Atlanta experienced major ransomware attacks resulting in disrupted government services [23, 76]. Energy facilities such as nuclear power plants are at risk to cyber attacks [65]; compromised energy facilities could result in major harm to the citizens who rely on their services. Data breaches within the healthcare industry are on the rise and can lead to patient identity theft [56], and the global average cost for companies to clean up after a data breach incident is $4M USD [32]. Shrinking the cybersecurity workforce gap is imperative to reducing the types of vulnerabilities outlined above.

Educational institutions have an important role to play in bolstering the cybersecurity workforce [52, 54, 64]. Increasing the number of cybersecurity programs and graduates with the knowledge, skills, and abilities (KSAs) necessary to perform cybersecurity jobs may address the workforce shortage and additionally decrease on-the-job training time [82]. As a result, governments are increasing funding for cybersecurity and the number of universities that offer degrees in cybersecurity is increasing [60, 81].

1.1 Cybersecurity Curricular Development

To guide the development of cybersecurity programs, multiple organizations have produced curricular guidelines. Whereas courses and course structure may vary between programs based on a department's focus or on faculty strengths, these curricula serve to create an overarching standard for which topics should be included across programs. In other words, cybersecurity curricula provide guidance as to what cybersecurity students need to know but do not dictate the specifics of how these topics should be taught.

Curricular guidelines may stem from designation or accreditation requirements. For example, to receive designation as a Center of Academic Excellence (CAE) from the National Security Administration, a program must demonstrate that it covers all core topics required by the designation and a certain number of discretionary topics [58]. ABET, a non-profit organization dedicated to accrediting STEM programs, recently unveiled accreditation criteria for undergraduate cybersecurity programs [1]. ABET's accreditation requirements were based on the post-secondary curricular guidelines put forth by the Joint Task Force on Cybersecurity Education.

The Task Force's curricular guidelines, referred to succinctly as CSEC2017, provide a list of over 250 topics related to cybersecurity [45]. These topics are organized into eight broad knowledge areas, each concerning one of the following security levels: (1) data, (2) software, (3) component, (4) connection, (5) system, (6) human, (7) organization, and (8) societal. Within each knowledge area are knowledge units, which are groups of topics.

CSEC2017 identifies 44 essential cybersecurity topics or knowledge areas that must be included in a curriculum in order for a student to have proficiency in cybersecurity. Those essentials address thefive characteristics that, according to the Task Force, all cybersecurity curricula should have:

(1) A computing-based foundation,
(2) Crosscutting concepts that are broadly applicable across the range of cybersecurity specializations,
(3) A body of knowledge containing essential cybersecurity knowledge and skills,

(4) A direct relationship to the range of specializations meeting the in-demand workforce domains, and
(5) A strong emphasis on the ethical conduct and professional responsibilities associated with thefield [45].

As mentioned above, CSEC2017 contains over 250 knowledge units and identifies only a percentage of them that should be included in all cybersecurity curricula. Thus, individual programs have a high degree of freedom in how they ful fi ll the curricular requirements as laid out in CSEC2017 (and by extension ABET) and also tailor their course offerings based on program goals and faculty strengths. Research has begun to examine the core concepts relevant to cybersecurity curricula [62], with plans to expand into specialized concepts [88].

In addition, CSEC2017 and the CAE accreditation requirements allow (but do not require) programs to develop specializations. Cybersecurity is a diversefield, so there are a large number of potential specializations [12, 25, 42, 71], and students may benefit from developing specializations during their training [41, 49]. How do programs that wish to offer cybersecurity specializations develop curricula for such specializations? To do so, programs mustfirst identify a target speciality area, preferably one that is in-demand. The proceeding section will discuss how programs can account for what is in-demand.

1.2 Accounting for What Is In-demand

According to CSEC2017, the fourth characteristic of an effective cybersecurity curricula is that there is "a direct relationship to the range of specializations meeting the in-demand workforce domains" [45]. Such a directive implies that academic program designers need both to understand what cybersecurity roles are in-demand and to understand the KSAs that students need to succeed in these roles. The knowledge of which roles are in-demand can be used to identify a program specialization, and the KSAs related to these roles can guide the development of a curriculum.

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework provides a taxonomy of cyber work as well as the KSAs required for said work [59]. Therefore, the NICE Framework may be used to help determine a program specialization and subsequently the KSAs relevant to that specialization. Indeed, the Framework is already widely used as a guide for program development [75] and evaluation [34]. The Framework is organized by types of cyber work. It identifies seven specialty areas within cybersecurity (Operate and Maintain, Protect and Defend, etc.), and for each a list of two to seven job types thatfit within the specialized domain. For example, there are four main job types within the Protect and Defend specialty area: Computer Network Defense Analysis (CNDA), Computer Network Defense Infrastructure Support (CNDIS), Incident Response (IR), and Vulnerability Assessment and Management (VAAM). An academic cybersecurity program may wish to specialize in Protect and Defend generally, and thereby focus on the KSAs relevant across job types within the Protect and Defend category or to specialize in one or a few of the specific job types and develop curricular requirements that prioritize the KSAs relevant to those job types [24].

To use the NICE Framework to fulfill the characteristics of an effective cybersecurity curricula, it is also necessary to determine which areas within the NICE Framework are in demand. If we can identify NICE framework roles that are in demand, then we will know what KSAs are needed to succeed in those roles. Cyber jobs with the highest demand include defense analysts, incident responders, and penetration testers [19, 20, 57], which fall under the Protect and Defend specialty area of the NICE Framework. Therefore, programs that wish to specialize within one area of cybersecurity would have good reason to focus on the Protect and Defend area and to prioritize teaching the KSAs utilized in Protect and Defend work.

Between two andfive dozen KSAs were listed under the four job types within the NICE Framework's Protect and Defend specialty area circa 2016 [77]. Many of these KSAs were shared between two or more of the job types and combined the Protect and Defend specialty area contained 79 unique KSAs. The topics of these KSAs spanned networks (e.g., knowledge of how trafficflows across the network, and skill in securing network communications), threats and vulnerabilities (e.g., ability to identify systemic security issues based on the analysis of vulnerability and configuration data, knowledge of system and application security threats and vulnerabilities), and many others (e.g., ability to interpret and incorporate data from multiple tool sources, knowledge of programming language structures and logic, and skill in the use of social engineering techniques).

1.3 Informing the Development of Protect and Defend Content for Specialized Curricula

Among the challenges in translating the KSAs from the NICE Framework into curricular guidelines are the difficulties involved with determining which KSAs should be prioritized. As mentioned above, the Protect and Defend specialty area contains 79 KSAs, and individual job types within the Protect and Defend specialty area may have as many as 61 KSAs [59]. Depending on their needs and abilities, a program may not wish to cover all KSAs that are used within certain cybersecurity jobs. The question becomes whether cyber professionals more frequently use some KSAs than others, or whether they otherwisefind some KSAs to be more important and others less important for their jobs. Such information would allow course and curriculum designers to prioritize KSAs from the NICE Framework according to industry needs. Unfortunately, the NICE Framework does not provide information as to whether some KSAs are more critical than others within a given line of work.

To address this gap, researchers have interviewed cybersecurity professionals and other subject matter experts on the cyber topics that should be addressed in education and training. It is recommended that curriculum developers regularly communicate with cyber professionals to ensure that course topics stay up to date and to otherwise enrich the curriculum [70, 71]. Depending on the unique goals of each research project, the interviewed experts may speak about cybersecurity topics generally [62, 69] or about speci fi c specialty areas within cybersecurity [4]. At least one study focused on professionals with Protect and Defend jobs [46].

In that study, 44 Protect and Defend professionals who attended the premier hacking conferences Black Hat or DEF CON rated the importance of 32 KSAs that were common to all four job types within the Protect and Defend category [46]. This information allows educators to prioritize which KSAs to include in their courses based on the relative importance of each KSA to the workforce. In addition, participants responded to a series of open-ended questions designed to identify additional KSAs that were important to Protect and Defend work. Their responses provided a list of 19 soft skills, coding languages, and technical knowledge that professionals deemed important for cybersecurity work but were not included in the NICE Framework.

The present study is a follow-up to previous research on cyber defense professionals [46]. In the present study, cybersecurity professionals working in one of the four main job types of the NICE Framework's Protect and Defend specialty area participated in a brief structured interview. Participants rated KSAs from the NICE Framework and those identified in previous research along two dimensions. First, the professionals rated how important each KSA was to their current job. Second, each participant rated how difficult each KSA was to learn.

The current study expanded on the previous interviews with Protect and Defend professionals [46] in three ways. First, the current research informs curricular development of programs that specialize in one of the four main job types within the Protect and Defend specialty area (CNDA, CNDIS, IR, and VAAM). Whereas previous research focused on the KSAs that were relevant across

Protect and Defend job types [46], the current study focused on the KSAs that are unique to each of the four main job types within the Protect and Defend speciality area. Second, the current research verified the importance of the KSAs identified during the previous interviews [46]. When asked whether there were additional KSAs that were important to their jobs, professionals provided a combined 19 responses. These 19 answers may point to additional KSAs that were not originally included in the NICE Framework, but that should be considered for cybersecurity curricula. Participants in the current study rated the importance of these 19 additional KSAs to their jobs, making it possible to verify whether these KSAs were relevant to Protect and Defend workers generally and not only to the subset of professionals that mentioned each KSA in the previous study. Third, the current study asked participants to rate how difficult it was for them to learn the KSAs included in their structured interviews. The NICE Framework and other curriculum standards and guidelines [62] provide very little guidance to educators who are making decisions about how to teach each KSA and how much course time to spend on each KSA. Thus, educators could benefit from information about the relative difficulty to learn each KSA.

2 METHOD

Methods were approved by the Institutional Review Board (IRB) at the researchers' home institution.

2.1 Procedure

Two researchers recruited participants at the Black Hat 2017 and DEF CON 25 cybersecurity conferences in Las Vegas, NV. The researchers followed the same procedure but worked independently. Researchers approached conference attendees and asked if they would be willing to participate in a short interview. If the attendee agreed, then they were shown a list of the four specialty areas within the Protect and Defend general knowledge area of the NICE Framework and asked which specialty area best described their job. The specialty areas were as follows: CNDA, CNDIS, IR, and VAAM. Structured interviews followed and were tailored to the participant's specialty area. Participants were informed they could skip any questions that they did not want to answer. Interviews generally lasted between 10 and 20 minutes.

2.2 Measures

The structured interviews began with questions that were common to all participants: 6 demographic questions and questions based on 19 KSAs common to all cyber defense professionals. The demographic questions were as follows: how many years they had been interested in cyber, how many years they had worked in a cybersecurity job, how many capture-the-flag events they had participated in, what was the highest level of education completed, their major (when applicable), and in which domain they worked (e.g., government, industry, or self-employed).

The 19 common KSAs were based on previous interviews with cyber defense professionals [46]. In that prior study, professionals listed all programming and soft skills that were important for their job, and whether there were any skills that were important to their job but that had not been covered by the previous questions, which concerned NICE KSAs. Nineteen unique KSAs were identified during this process. These were KSAs, including but not limited to non-technical KSAs, that cyber defense professionals reported as being important to their work but that had not been included in the NICE Framework. A full list of these KSAs can be found in Table 1. In the present study, participants were asked two questions about each KSA. Thefirst question was "How important is [this KSA] for your job on a scale of one to six?" Participants responded along a 6-point scale anchored such that 1 = "not important at all" and 6 = "very important." The second question

was, "How difficult was it to learn [this KSA] on a scale of one to six?" Participants responded along a 6-point scale anchored such that 1 = "not at all difficult" and 6 = "very difficult."

Following the demographic questions and common KSAs, participants were asked about KSAs specific to their specialty area (CNDA, CNDIS, IR, or VAAM). These KSAs were taken from the NICE Framework circa 2016. In previous interviews with cyber defense professionals [46], participants were interviewed about 32 KSAs that were listed as necessary for two or more of the four Protect and Defend specialty areas. For the current study, interviews consisted of the NICE KSAs that were not included in the previous research effort [46]. Depending on participant specialty area, interviews contained 8 to 34 KSAs from the NICE Framework. A full list of NICE KSAs used can be found in Tables 2–6. As with the common KSAs, participants indicated the importance of each KSA to their job and the extent to which the KSA was difficult for them to learn.

All structured interviews concluded with two open-ended questions. First, participants were asked which of the KSAs they considered to be the most important for novices in their specialty area. Second, participants were encouraged to comment on anything they wished the researchers to know to strengthen the education and training of novices in theirfield.

2.3 Participants

Participants were 48 cybersecurity professionals. There are four specialty areas within the NICE Framework's Protect and Defend general knowledge area: CNDA, CNDIS, IR, and VAAM. Fifteen participants worked in CNDA (31%), 10 in CNDIS (21%), 3 in IR (6%), and 20 in VAAM (42%). The majority of the participants (29) worked in industry (60%), 9 worked for the government (19%), 2 were self-employed (4%), and 4 worked for some combination of the above (8%). An additional 4 participants did not respond or did notfit into any of the above categories (8%). Those participants who chose to self-disclose more information about their employment indicated that they worked withing the medical, telecommunications, and consulting industries.

On average, participants had held a job utilizing cybersecurity knowledge and skills for 8.47 years ($SD = 6.81$; range = 0.15–32 years), had been interested in cyber for 12.66 years ($SD = 9.22$; range: 1–43 years), and had participated in 5.27 capture-the-flag events ($SD = 16.92$; range: 0–100 events). The highest degree attained was a high school diploma or GED for 7 participants (15%), an associates for 2 (4%), a bachelors for 21 (44%), and a postgraduate for 18 (38%). Of the professionals interviewed who completed post-secondary education, the most common majors were computer science ($n = 13$), computer engineering ($n = 7$), and cybersecurity ($n = 6$). Participants' amount of work experience and educational background is comparable to the samples used in other studies of cybersecurity professionals [39, 74, 79].

High school graduates and GED holders had worked in cybersecurity for a little over 8 years on average ($M = 8.21$, $SD = 7.26$, range: 3.5–24). The two participants with associate degrees had each been in thefield for around two decades ($M = 19.50$, $SD = 2.12$). Similarly to the high school graduates, participants with bachelors and with postgraduate degrees had on average worked in cybersecurity for about 8 years (bachelors: $M = 7.85$, $SD = 5.69$, range: 2 months to 20 years; postgraduate: $M = 8.06$, $SD = 7.50$, range: 1 to 32 years). Based on a series of one-way ANOVAs with education level as the independent variable, there was no reason to conclude that participants differed significantly between degree types in years of cyber work experience, $F(3, 44) = 0.79$, $p = 0.505$, years of interest in cybersecurity, $F(3, 44) = 0.63$, $p = 0.597$, or in capture-the-flag participation $F(3, 42) = 0.02$, $p = 0.995$.

2.4 Data Analysis

For each KSA, we calculated mean ratings of importance and difficulty to learn. Because participants rated each KSA along 6-point continuous scales, the neutral point of the scales was 3.5. To

determine whether KSAs were rated as being significantly above or below neutral, we performed a series of bootstrap analyses.

Our decision to use bootstrapping reflected that we had small sample sizes when analyzing the mean ratings of specialty area KSAs. More traditional analyses, such as the t-test or Wilcoxon Signed-Rank test, are not ideal for smaller sample sizes, because they rely on assumptions of normality or lack statistical power [90]. The bootstrap provides a non-parametric way of assessing whether a population mean is significantly different from a given value. Accordingly, bootstrap analysis is well suited for sample sizes under 30 [5, 90] and can be used with sample sizes as low as 9 [6, 7, 31, 61]. For subsets of our population where $n \geq 9$, we employed the bootstrap procedure. For one participant subset, the IR group, $n < 9$, so we did not perform any inferential analyses on the IR subset.

For the importance ratings and the difficulty to learn ratings of each KSA, we randomly resampled the observed data with replacement 10,000 times. This resulted in 10,000 simulations of the data and a mean rating for each simulation. The simulated means provide a distribution of the mean ratings, and this distribution was used tofind a confidence interval (CI) around each mean rating.

When the lower limit of a CI fell above 3.5, the neutral point of the importance scale, we concluded that participants rated the associated KSAs as relatively important. When the CI overlapped with 3.5, we concluded that participants rated the associated KSA as neither relatively important nor unimportant (neutral). When the upper limit of a CI fell below the neutral point, we concluded that participants rated the associated KSA as relatively unimportant. Similarly, for ratings of how difficult a KSA was to learn, when the lower limit of a CI was above the neutral point of the scale (3.5), we concluded that the associated KSA was relatively difficult to learn. When the CI overlapped with 3.5, we concluded that the associated KSA was neither relatively difficult nor easy to learn (neutral), and when the upper limit of the CI was less than 3.5, we concluded that the associated KSA was relatively easy to learn.

Bootstrap analyses typically work with an α value of .05, which corresponds to a 95% CI. To ward against Type I error, we elected to use a Bonferroni correction and hold an α value of .05 for each group of KSAs. The common KSAs were considered one group, the CNDA KSAs a second group, and so on. For each KSA within a group, the α level was equal to .05 divided by the total number of KSAs within the group. This corrected α level was used to determine the size of the CIs found for each group of KSAs. As a result, a 99% CI was found for each KSA, resulting in a more conservative test of significance. Exact percentile values used in the 99% CIs are reported with the tables.

Finally, Pearson's r was calculated to determine whether mean importance ratings correlated with mean difficulty ratings. Separate calculations were conducted for each specialty area.

3 RESULTS

3.1 Which Common KSAs Should Be Prioritized in Cyber Defense Education?

For both importance and difficulty to learn ratings, bootstrapped confidence intervals were computed to compare participants' ratings of the 19 common KSAs to a neutral rating of 3.5 (Table 1). The alpha level used to compute these confidence intervals was $\alpha = .05/19 = .003$.

Inspection of Table 1 reveals that the bootstrapped confidence intervals for 12 of the 19 common KSAs fell above the importance scale's neutral point (KSAs 1–12), those for 3 of the 19 common KSAs overlapped with the importance scale's neutral point (KSAs 13–15), and those for 4 of the 19 common KSAs fell below the importance scale's neutral point (KSAs 16–19). Accordingly, KSAs 1–12 were rated as relatively important, and KSAs 16–19 were rated as relatively unimportant.

Table 1. Importance and Difficulty to Learn of the KSAs Common to All Cyber Defense Professionals

	Importance to Job Ratings						Difficulty to Learn Ratings					
	Observed Statistics			Bootstrapped Statistics			Observed Statistics			Bootstrapped Statistics		
					99% CI						99% CI	
Knowledge, Skills, and Abilities	n	M_{obs}	SD	M_{boot}	LL	UL	n	M_{obs}	SD	M_{boot}	LL	UL
1. Ability to be curious	47	5.51	0.86	5.51	5.06	5.85	47	2.53	1.61	2.53	1.87	3.32
2. Skill in collaborating with the people you work with	47	5.49	0.86	5.49	5.11	5.81	47	3.34	1.34	3.34	2.77	3.94
3. Skill in stay motivated	47	5.47	0.97	5.47	5.00	5.83	47	3.36	1.62	3.36	2.68	4.06
4. Knowledge of current events and changes within yourfield	47	5.45	0.85	5.45	5.04	5.77	47	3.02	1.15	3.02	2.55	3.53
5. Skill in written communication (e.g., technical reports)	47	5.40	0.88	5.40	5.00	5.74	47	3.68	1.35	3.68	3.09	4.28
6. Ability to be adaptable	47	5.36	0.79	5.36	5.00	5.68	47	2.91	1.46	2.91	2.32	3.57
7. Skill in communication with clients or users	47	5.28	1.31	5.28	4.66	5.77	46	3.48	1.38	3.48	2.89	4.07
8. Skill in communication with management	47	5.28	1.04	5.28	4.83	5.66	47	3.70	1.49	3.70	3.09	4.30
9. Skill in researching and using search engines	47	5.11	1.15	5.11	4.57	5.57	47	2.17	0.99	2.17	1.74	2.60
10. Knowledge of operating systems	47	5.00	1.43	5.00	4.34	5.55	47	3.83	1.26	3.83	3.28	4.34
11. Knowledge of logic and logic structures	47	4.49	1.47	4.49	3.81	5.09	47	3.09	1.19	3.08	2.57	3.64
12. Knowledge of packet-analysis	47	4.43	1.58	4.42	3.70	5.04	46	3.85	1.30	3.85	3.26	4.39
13. Skill in coding in Python	47	3.96	1.84	3.95	3.15	4.76	46	3.26	1.39	3.26	2.68	3.89
14. Knowledge of reverse engineering	47	3.94	1.77	3.94	3.15	4.68	45	4.76	1.46	4.76	4.07	5.36
15. Skill in coding in Java	47	2.81	1.84	2.80	2.06	3.60	43	3.67	1.44	3.68	3.00	4.30
16. Skill in coding in C++	47	2.72	1.62	2.72	2.06	3.40	43	4.12	1.38	4.11	3.42	4.72
17. Knowledge of electrical engineering	47	2.45	1.74	2.45	1.72	3.21	43	3.95	1.62	3.96	3.21	4.63
18. Skill in coding in Ruby	47	2.36	1.61	2.37	1.70	3.09	42	3.19	1.47	3.19	2.52	3.86
19. Skill in coding in Perl	47	2.34	1.54	2.34	1.74	3.02	42	3.74	1.43	3.74	3.07	4.36

Note: KSAs are listed by mean importance rating, from highest to lowest. Listed under both the Importance to Job and Difficulty to Learn columns are number of respondents (n), observed mean rating (M_{obs}), standard deviation of observed rating (SD), the bootstrapped mean rating (M_{boot}), and the lower limit (LL) and upper limit (UL) of the 99% Confidence Interval. For this group of KSAs, the confidence interval represents the 0.13 and the 99.87 percentiles.

Further inspection of Table 1 reveals that the bootstrapped confidence intervals for 1 of the 19 common KSAs fell above the difficulty scale's neutral point (KSA 14), those for 16 of the 19 common KSAs overlapped with the difficulty scale's neutral point (KSAs 2–8, 10–13, and 15–19), and those for 2 of the 19 common KSAs fell below the difficulty scale's neutral point (KSAs 1 and 9). Therefore, KSA 14 was rated as relatively difficult to learn, and KSAs 1 and 9 were rated as relatively easy to learn; all other common KSAs were considered neither difficult nor easy to learn. The correlation between participants' importance and difficulty ratings of the 19 common KSAs was not statistically significant $r(17) = -.42, p = 0.073$.

3.1.1 Knowledge. Four knowledge topics were rated as relatively important, including the knowledge of current events and changes in thefield (KSA 4), operating systems (KSA 10), logic and logic structures (KSA 11), and packet-analysis (KSA 12). One knowledge topic was rated as neither relatively important nor unimportant (neutral), i.e., the knowledge of reverse engineering

(KSA 14). One knowledge topic was rated as relatively unimportant, i.e., the knowledge of electrical engineering (KSA 17).

3.1.2 Skills. Six skills were rated as relatively important, including communication skills (KSAs 2, 5, 7, and 8), staying motivated (KSA 3), and researching and using search engines (KSA 9). Two skills were rated as neither relatively important nor unimportant (neutral), including Python and Java (KSAs 13 and 15). Three skills were rated as relatively unimportant, including C++, Ruby, and Perl (KSAs 16, 17, and 18).

3.1.3 Abilities. Two abilities were rated as relatively important, including the ability to be curious (KSA 1) and the ability to be adaptable (KSA 6). No abilities were rated as neutral or as relatively unimportant.

3.2 Which KSAs Are Needed by CNDA Professionals?

For both importance and difficulty to learn ratings, bootstrapped confidence intervals were computed to compare participants' ratings of the 34 KSAs that were unique to the CNDA specialty area to a neutral rating of 3.5 (Tables 2 and 3). The alpha level used to compute these confidence intervals was $\alpha = .05/34 = .001$.

Inspection of Table 2 reveals that the bootstrapped confidence intervals for 17 of the 34 KSAs fell above the importance scale's neutral point (KSAs 20–31, 33–35, and 37 and 38), and those for 17 of the 34 KSAs overlapped with the importance scale's neutral point (KSAs 32, 36, and 39–53). Accordingly, KSAs 20–31, 33–35, and 37–38 were rated as relatively important, the others were rated as neither important nor unimportant, and no KSAs unique to CNDA were rated as relatively unimportant. Further inspection of Table 2 reveals that the bootstrapped confidence intervals for 34 of the 34 KSAs overlapped with the difficulty scale's neutral point (KSAs 20–53). Therefore, no KSAs were rated as relatively difficult or easy to learn. The correlation between participants' importance and difficulty ratings of the 34 KSAs that were unique to the CNDA specialty area was not statistically significant, $r(32) = .22$, $p = 0.211$.

3.2.1 Knowledge. Fifteen knowledge topics unique to the CNDA specialty area were rated as relatively important, including knowledge of networks and network tools (KSAs 20, 23, 26, 29, and 30), adversaries and attacks (KSAs 21, 25), data collection and interpretation (KSAs 33 and 38), network defense and security (KSAs 24, 34, 35, and 37), new and emerging security technologies (KSA 27), andfile extensions (KSA 28). Five knowledge topics were rated as neither relatively important nor unimportant (neutral), including knowledge about encryption (KSA 39 and 41), the Windows command line (KSA 43), applicable laws (KSA 46), signature implementation (KSA 47), and computer network defense service providers' report structure and process (KSA 51). No knowledge topics were rated as relatively unimportant.

3.2.2 Skills. One skill unique to the CNDA specialty area was rated as relatively important, i.e., skill in collecting data from a variety of computer network defense resources (KSA 31). Eleven skills unique to the CNDA specialty area were rated as neither relatively important nor unimportant (neutral), including skills related to using various tools (KSA 36, 40, 44, and 50), working with data (KSAs 49 and 52), dealing with signatures (KSAs 48 and 53), conducting open-source research for troubleshooting novel client problems (KSA 32), network mapping and recreating network topologies (KSA 42), and identifying common encoding techniques (KSA 45). No skills were rated as relatively unimportant.

Table 2. Importance and Difficulty to Learn of Computer Network Defense Analysis KSAs—Part 1

	Importance to Job Ratings						Difficulty to Learn Ratings					
	Observed Statistics			Bootstrapped Statistics			Observed Statistics			Bootstrapped Statistics		
					99% CI						99% CI	
Knowledge, Skills, and Abilities	n	M_{obs}	SD	M_{boot}	LL	UL	n	M_{obs}	SD	M_{boot}	LL	UL
20. Knowledge of common network tools	15	5.53	0.92	5.54	4.73	6.00	15	2.73	1.28	2.74	1.89	3.87
21. Knowledge of common adversary tactics, techniques, and procedures in assigned area of responsibility	15	5.47	1.06	5.47	4.56	6.00	15	4.27	1.75	4.27	2.80	5.53
22. Ability to interpret and incorporate data from multiple tool sources	15	5.40	0.63	5.40	4.87	5.87	15	4.13	1.55	4.13	2.87	5.27
23. Knowledge of different types of network communication	15	5.13	1.36	5.13	3.89	5.93	15	3.60	1.59	3.60	2.33	4.84
24. Knowledge of Defense-In-Depth principles and network security architecture	15	5.07	1.33	5.07	3.87	5.84	14	4.07	1.38	4.07	3.00	5.21
25. Knowledge of the common attack vectors on the network layer	15	5.07	1.16	5.07	4.00	5.80	15	3.73	1.44	3.73	2.62	4.80
26. Knowledge of unix command line	15	5.07	1.53	5.06	3.69	5.91	15	3.07	1.28	3.07	2.13	4.20
27. Knowledge of new and emerging IT and information security technologies	15	5.00	1.41	5.00	3.73	5.93	15	3.53	1.41	3.53	2.53	4.60
28. Knowledge offile extensions	15	4.93	1.62	4.94	3.53	5.93	15	2.27	1.33	2.26	1.47	3.53
29. Knowledge of windows and unix ports and services	15	4.93	1.39	4.93	3.62	5.73	15	2.60	1.18	2.60	1.73	3.53
30. Knowledge of troubleshooting basic systems and operating system related issues	15	4.87	1.41	4.87	3.60	5.73	15	3.33	1.45	3.33	2.27	4.47
31. Skill in collecting data from a variety of Computer Network Defense resources	15	4.87	1.19	4.86	3.89	5.67	15	3.47	1.51	3.47	2.29	4.67
32. Skill in conducting open-source research for troubleshooting novel client problems	15	4.87	1.51	4.87	3.47	5.73	14	3.00	1.36	3.00	2.00	4.14
33. Knowledge of collection management processes, capabilities, and limitations	15	4.80	1.08	4.80	3.87	5.53	15	3.93	1.44	3.93	2.82	5.04
34. Knowledge of Computer Network Defense and vulnerability assessment tools, including open source tools, and their capabilities	15	4.73	1.28	4.73	3.67	5.67	15	3.20	1.37	3.20	2.13	4.20
35. Knowledge of security management	15	4.73	1.16	4.73	3.67	5.53	15	3.33	0.98	3.33	2.53	4.07

Note: Table continued on following page.

3.2.3 Abilities. One ability unique to the CNDA specialty area was rated as relatively important, i.e., the ability to interpret and incorporate data from multiple tools (KSA 22). No KSAs were rated as neutral or as unimportant.

3.3 Which KSAs Are Needed by CNDIS Professionals?

For both importance and difficulty to learn ratings, bootstrapped confidence intervals were computed to compare participants' ratings of the 8 KSAs that were unique to the CNDIS specialty area to a neutral rating of 3.5 (Table 4). The alpha level used to compute these confidence intervals was $\alpha = .05/8 = .006$.

Table 3. Importance and Difficulty to Learn of Computer Network Defense Analysis KSAs—Part 2

	Importance to Job Ratings						Difficulty to Learn Ratings					
	Observed Statistics			Bootstrapped Statistics			Observed Statistics			Bootstrapped Statistics		
					99% CI						99% CI	
Knowledge, Skills, and Abilities	n	M_{obs}	SD	M_{boot}	LL	UL	n	M_{obs}	SD	M_{boot}	LL	UL
36. Skill in utilizing virtual networks for testing	15	4.73	1.87	4.73	3.09	5.87	15	2.93	1.03	2.93	2.13	3.73
37. Knowledge of policy-based and risk adaptive access controls	15	4.67	1.35	4.67	3.53	5.60	15	3.27	1.10	3.27	2.53	4.20
38. Knowledge of front-end collection systems	15	4.60	1.35	4.60	3.53	5.60	15	3.47	1.41	3.46	2.40	4.58
39. Knowledge of cryptology	15	4.53	1.55	4.53	3.13	5.60	15	4.07	1.62	4.07	2.87	5.33
40. Skill in configuring and utilizing network protection components	15	4.53	2.00	4.54	2.93	5.87	14	3.86	1.70	3.86	2.45	5.29
41. Knowledge of encryption methodologies	15	4.47	1.55	4.47	3.29	5.53	15	4.20	1.66	4.20	2.93	5.47
42. Skill in network mapping and recreating network topologies	15	4.47	1.92	4.47	2.82	5.73	14	3.71	1.68	3.72	2.36	5.07
43. Knowledge of windows command line	15	4.13	2.10	4.13	2.33	5.58	15	2.60	1.12	2.60	1.80	3.53
44. Skill in using protocol analyzers	14	4.07	1.27	4.07	3.00	4.93	14	3.71	1.59	3.71	2.36	4.86
45. Skill in identifying common encoding techniques	15	4.07	1.98	4.06	2.36	5.47	15	3.27	1.33	3.27	2.16	4.20
46. Knowledge of applicable laws	15	3.93	1.67	3.94	2.67	5.20	15	3.67	1.84	3.66	2.27	5.07
47. Knowledge of signature implementation impact	14	3.71	1.64	3.71	2.36	4.86	13	2.92	1.32	2.92	2.00	4.13
48. Skill in reading and interpreting signatures	15	3.53	1.88	3.54	2.20	4.98	14	4.07	1.44	4.07	2.88	5.14
49. Skill in data reduction	15	3.47	2.23	3.46	1.80	5.13	14	2.64	1.50	2.64	1.57	4.00
50. Skill in using sub netting tools	15	3.47	2.13	3.47	1.87	5.07	13	2.62	1.12	2.61	1.69	3.62
51. Knowledge of the computer network defense service provider reporting structure and process within one	14	3.43	1.83	3.43	2.00	4.86	12	3.67	1.61	3.67	2.45	5.08
52. Skill in reading hexadecimal data	15	3.27	2.02	3.27	1.67	4.84	15	3.07	1.62	3.07	1.87	4.33
53. Skill in developing and/or deploying signatures	14	2.86	1.61	2.86	1.71	4.24	13	2.92	1.44	2.93	1.72	4.15

Note: KSAs are listed by mean importance rating, from highest to lowest. Listed under both the Importance to Job and Difficulty to Learn columns are number of respondents (n), observed mean rating (M_{obs}), standard deviation of observed rating (SD), the bootstrapped mean rating (M_{boot}), and the LL and UL of the 99% Confidence Interval. For this group of KSAs, the confidence interval represents the 0.07 and the 99.93 percentiles.

Inspection of Table 4 reveals that the bootstrapped confidence intervals for 1 of the 8 KSAs fell above the importance scale's neutral point (KSA 54), those for 6 of the 8 KSAs overlapped with the importance scale's neutral point (KSAs 55–60), and those for 1 of the KSAs fell below the importance scale's neutral point (KSA 61). Accordingly, KSA 54 was rated as relatively important, and KSA 61 was rated as relatively unimportant. Further inspection of Table 4 reveals that the bootstrapped confidence intervals for 8 of the 8 KSAs overlapped with the difficulty scale's neutral point (KSAs 54–61). Therefore, no KSAs were rated as relatively difficult or easy to learn. The correlation between participants' importance and difficulty ratings of the 34 KSAs that were unique to the CNDA specialty area was not statistically significant, $r(6) = .26$, $p = 0.534$.

Table 4. Importance and Difficulty to Learn of Computer Network Defense Infrastructure Support KSAs

	Importance to Job Ratings						Difficulty to Learn Ratings					
	Observed Statistics			Bootstrapped Statistics			Observed Statistics			Bootstrapped Statistics		
					99% CI						99% CI	
Knowledge, Skills, and Abilities	n	M_{obs}	SD	M_{boot}	LL	UL	n	M_{obs}	SD	M_{boot}	LL	UL
54. Knowledge of the types of intrusion detection software and hardware	10	5.10	1.60	5.09	3.60	6.00	10	3.80	1.48	3.80	2.70	5.10
55. Skill in using VPN devices and encryption	9	4.33	2.06	4.34	2.44	5.78	8	3.50	1.69	3.51	2.00	5.00
56. Knowledge of processes for reporting network security related incidents	10	4.30	1.89	4.30	2.60	5.60	9	2.56	1.24	2.55	1.56	3.67
57. Knowledge of web-filtering technologies	10	4.30	1.95	4.30	2.52	5.60	9	3.33	1.22	3.33	2.22	4.22
58. Knowledge of transmission methods	9	4.00	1.87	4.01	2.33	5.44	9	3.89	1.76	3.89	2.33	5.33
59. Skill in tuning sensors	10	3.60	2.41	3.59	1.70	5.40	7	3.57	1.99	3.57	1.57	5.29
60. Knowledge of CMMI	9	2.33	1.41	2.34	1.22	3.67	6	3.50	0.55	3.50	3.00	4.00
61. Knowledge of voice over IP	10	2.20	1.23	2.20	1.30	3.20	9	2.89	1.27	2.90	1.89	4.00

Note: KSAs are listed by mean importance rating, from highest to lowest. Listed under both the Importance to Job and Difficulty to Learn columns are number of respondents (n), observed mean rating (M_{obs}), standard deviation of observed rating (SD), the bootstrapped mean rating (M_{boot}), and the LL and UL of the 99% Confidence Interval. For this group of KSAs, the confidence interval represents the 0.31 and the 99.69 percentiles.

It is worth noting that many participants declined to rate how difficult it was for them to learn the CNDIS KSAs. As a result, the sample sizes for some of the KSA difficulty ratings are arguably too small for the bootstrap test to be accurate. Accordingly, thefindings concerning difficulty to learn should be interpreted cautiously.

3.3.1 Knowledge. One knowledge topic unique to the CNDIS specialty area was rated as relatively important, i.e., knowledge of types of intrusion detection software and hardware (KSA 54). Four knowledge topics were rated as neither relatively important nor unimportant (neutral), including knowledge about processes of reporting network security related incidents (KSA 56), Webfiltering technologies (KSA 57), transmission methods (KSA 58), and CMMI (KSA 60). One knowledge topic was rated as relatively unimportant, i.e., knowledge of voice-over-IP (KSA 61).

3.3.2 Skills. No skills unique to the CNDIS specialty area were rated as relatively important or relatively unimportant. Two skills were rated as neither relatively important nor unimportant (neutral), including skill in using VPN devices and encryption (KSA 55) and skill in tuning sensors (KSA 59).

3.3.3 Abilities. There were no abilities unique to the CNDIS specialty area.

3.4 Which KSAs Are Needed by IR Professionals?

Only three participants reported working within the IR specialty area, so it was not appropriate to compute bootstrapped confidence intervals for this group of KSAs. Therefore, Table 5 presents only observed means and standard deviations for these KSAs.

In the following, we note whether the observed means were above or below the importance and difficulty scales' neutral points, so as to provide some interpretation of the data related to the IR specialty area. However, these notes should be considered preliminary given that it was not possible to determine statistical significance.

Table 5. Importance and Difficulty to Learn of Incident Response KSAs

	Importance to Job Ratings			Difficulty to Learn Ratings		
Knowledge, Skills, and Abilities	n	M_{obs}	SD	n	M_{obs}	SD
62. Knowledge of incident categories, incident responses, and timelines for responses	3	5.67	0.58	3	4.33	0.58
63. Knowledge of how network services and protocols interact to provide network communications	3	5.67	0.58	3	3.00	0.00
64. Skill in handling malware	3	5.33	0.58	3	4.33	1.53
65. Skill in preserving evidence integrity according to standard operating procedures or national standards	3	4.67	1.15	3	3.00	1.00
66. Knowledge of security event correlation tools	3	4.67	1.53	3	4.33	1.53
67. Knowledge of malware analysis concepts and methodology	3	4.67	2.31	3	4.33	2.08

KSAs are listed by mean importance rating, from highest to lowest. Listed under both the Importance to Job and Difficulty to Learn columns are number of respondents (n), observed mean rating (M_{obs}), and standard deviation of observed rating (SD).

Inspection of Table 5 reveals that means for 6 of the 6 KSAs unique to the IR specialty area fell above the importance scale's neutral point (KSAs 62–67). Accordingly, KSAs 62–67 were rated as relatively important. Further inspection of Table 5 reveals that the means for (a) 4 of the KSAs fell above the difficulty scale's neutral point (KSAs 62, 64, 66, and 67), and (b) 2 of the KSAs fell below the difficulty scale's neutral point (KSAs 63 and 65). Therefore, KSAs 62, 64, 66, and 67 were rated as relatively difficult to learn and KSAs 63 and 65 were rated as relatively easy to learn.

3.4.1 Knowledge. Four knowledge topics unique to the IR specialty area were rated as relatively important, including knowledge of incidents (KSA 62), networks (KSA 63), tools (KSA 66), and malware (KSA 67).

3.4.2 Skills. Two skills unique to the IR specialty area were rated as relatively important, including skill in handling malware (KSA 64) and skill in preserving evidence integrity (KSA 65).

3.4.3 Abilities. There were no abilities unique to the IR specialty area.

3.5 Which KSAs Are Needed by VAAM Professionals?

For both importance and learning difficulty ratings, bootstrapped confidence intervals were computed to compare participants' ratings of the 13 KSAs that were unique to the VAAM specialty area to a neutral rating of 3.5 (Table 6). The alpha level used to compute these confidence intervals was $\alpha = .05/13 = .004$.

Inspection of Table 6 reveals that the bootstrapped confidence intervals for 7 of the 13 KSAs fell above the importance scale's neutral point (KSAs 68–74), and those for 6 of the 13 KSAs overlapped with the importance scale's neutral point (KSAs 75–80). Accordingly, KSAs 68–74 were rated as relatively important, and no KSAs were rated as relatively unimportant. Further inspection of Table 6 reveals that the bootstrapped confidence intervals for (a) 1 of the 13 KSAs fell above the difficulty scale's neutral point (KSA 70), and (b) 12 of the 13 KSAs overlapped with the difficulty scale's neutral point (KSAs 68, 69, and 71–80). Therefore, 1 KSA was rated as relatively difficulty to learn, and no KSAs were rated as relatively easy to learn. The correlation between participants' importance and difficulty ratings of the 13 KSAs that were unique to the VAAM specialty area

Table 6. Importance and Difficulty to Learn of Vulnerability Assessment and Management KSAs

	Importance to Job Ratings						Difficulty to Learn Ratings					
	Observed Statistics			Bootstrapped Statistics			Observed Statistics			Bootstrapped Statistics		
					99% CI						99% CI	
Knowledge, Skills, and Abilities	n	M_{obs}	SD	M_{boot}	LL	UL	n	M_{obs}	SD	M_{boot}	LL	UL
68. Knowledge of system and application security threats and vulnerabilities	20	5.30	0.98	5.30	4.60	5.80	20	3.80	0.83	3.80	3.25	4.30
69. Ability to identify systemic security issues based on the analysis of vulnerability and configuration data	19	5.16	1.38	5.15	4.12	5.89	19	3.79	1.03	3.79	3.11	4.37
70. Skill in the use of penetration testing tools and techniques	19	5.11	1.49	5.11	4.05	5.95	19	4.32	1.11	4.31	3.58	5.00
71. Knowledge of application vulnerabilities	20	5.05	1.32	5.05	4.15	5.75	20	3.90	1.17	3.90	3.10	4.55
72. Knowledge of system diagnostic tools and fault identification techniques	20	4.95	1.39	4.95	4.00	5.70	19	3.58	0.96	3.58	2.95	4.20
73. Skill in assessing the robustness of security systems and designs	19	4.95	1.27	4.95	4.05	5.68	19	4.11	1.05	4.10	3.47	4.78
74. Knowledge of network access, identity, and access management	20	4.50	1.36	4.50	3.60	5.25	20	3.75	1.07	3.75	3.10	4.40
75. Knowledge of interpreted and compiled computer languages	20	4.30	1.69	4.30	3.20	5.25	20	3.70	1.13	3.70	3.00	4.40
76. Skill in mimicking threat behaviors	19	4.21	1.58	4.21	3.12	5.11	18	4.11	1.02	4.11	3.50	4.83
77. Knowledge of local and specialized system requirements	20	4.10	1.68	4.10	3.05	5.14	19	3.42	1.02	3.43	2.74	4.04
78. Knowledge of relevant laws, policies, procedures, and governance as they relate to work that may impact critical infrastructure	20	3.85	1.95	3.85	2.55	5.10	18	3.78	1.11	3.78	3.11	4.61
79. Skill in evaluating the trustworthiness of the supplier and/or product	19	3.79	1.72	3.79	2.68	4.84	19	3.42	1.43	3.42	2.47	4.32
80. Skill in the use of social engineering techniques	19	3.37	1.89	3.37	2.11	4.58	17	3.41	1.84	3.41	2.18	4.63

Note: KSAs are listed by mean importance rating, from highest to lowest. Listed under both the Importance to Job and Difficulty to Learn columns are number of respondents (n), observed mean rating (M_{obs}), standard deviation of observed rating (SD), the bootstrapped mean rating (M_{boot}), and the LL and UL of the 99% Confidence Interval. For this group of KSAs, the confidence interval represents the 0.07 and the 99.93 percentiles.

was statistically significant and positive, $r(11) = .57$, $p = 0.042$, which indicates that KSAs rated as being more important to VAAM jobs also tended to be rated as more difficult to learn.

3.5.1 Knowledge. Four knowledge topics unique to the VAAM specialty area were rated as relatively important, including knowledge of vulnerabilities (KSAs 68 and 71), system diagnostic tools (KSA 72), and networks (KSA 74). Three knowledge topics were rated as neither relatively important nor unimportant (neutral), including knowledge of interpreted and compiled computer languages (KSA 75), local and specialized system requirements (KSA 77) and relevant laws, policies, and so on that relate to critical infrastructure (KSA 78). No knowledge topics were rated as relatively unimportant.

3.5.2 Skills. Two skills unique to the VAAM specialty area were rated as relatively important, including skills related to use of penetration testing tools and techniques (KSA 70) and assessing the robustness of security systems and designs (KSA 73). Three skills were rated as neither important nor unimportant (neutral), including skills related to mimicking threat behavior (KSA 76),

evaluating supplier and/or product trustworthiness (KSA 79), and use of social engineering techniques (KSA 80). No skills were rated as relatively unimportant.

3.5.3 Abilities. One ability was rated as relatively important, i.e., the ability to identify systemic security issues based on the analysis of vulnerability and configuration data (KSA 69). No abilities were rated as neither important nor unimportant (neutral), or as relatively unimportant.

4 DISCUSSION

The present study was designed to provide educators with information that would help them develop specialized cybersecurity curricula. We interviewed cybersecurity professionals who worked in one of four specializations within cyber defense (CNDA, CNDIS, IR, and VAAM) to assess which KSAs are currently in-demand. The cybersecurity professionals rated the extent to which each KSA was important to their job and difficult to learn. The KSAs included 19 found in previous research efforts [46] that were anticipated to be important to all cyber defense professionals. Additionally, each participant rated KSAs from the NICE Framework that were unique to their specialty area within cyber defense.

Using a bootstrap resampling procedure, we computed confidence intervals for each KSA's importance and difficulty ratings. When the confidence interval fell above the importance or difficulty scales' neutral points (3.5), we concluded that participants rated the associated KSA as relatively important. When the CI overlapped with those scales' neutral points, we concluded that participants rated the associated KSA as neither relatively important or unimportant (neutral). When the confidence interval fell below those scales' neutral points, we concluded that participants rated the associated KSA was relatively unimportant.

To be clear, it is not our intention that thesefindings serve as a binary decision-making guide whereby, for example, all KSAs that were rated as relatively important are automatically included in cyber defense curricula and all others are not. Rather, we expect that thesefindings will be useful in that, all else being equal, educators can prioritize KSAs based on rated importance, with KSAs rated as relatively important being prioritized the highest. We make suggestions for the inclusion of specialty KSAs in the sections below.

Once educators have decided to include a KSA in their curriculum, they mayfind it valuable to know how difficult it was for cybersecurity professionals to learn that KSA. Those professionals' experiences provide some insight into how difficult it may be for students to learn that KSA. Educators may wish to use this information to estimate the amount of time or assistance students will need to gain competency in a KSA [37, 62]. That said, how difficult it is to learn a given KSA should not influence decisions regarding whether to include that KSA in specialized curricula. Accordingly, our discussion will focus on how important KSAs were to cybersecurity professionals' jobs and not on how difficult it was for those professionals to learn the KSAs.

4.1 Teaching KSAs Common to All Cyber Defense Careers

4.1.1 Knowledge. Of the six knowledge topics that participants rated, four were rated as relatively important: knowledge of current events and changes in thefield (KSA 4), knowledge of operating systems (KSA 10), knowledge of logic and logic structures (KSA 11), and knowledge of packet-analysis (KSA 12). Knowledge of reverse engineering (KSA 14) was rated as neither relatively important nor relatively unimportant (neutral), and knowledge of electrical engineering (KSA 17) was rated as relatively unimportant.

Knowledge of topics such as current events and operating systems is more general than knowledge of reverse engineering or electrical engineering. The latter types of knowledge may be important for some, but not all, types of cyber defense work. Past research has found that expert

ratings of topic importance strongly correlate with their ratings of timelessness [62]. Thus, it may be that the more important knowledge topics are more timeless, whereas the utility of other types of knowledge may be more ephemeral.

Current events are by definition not timeless; therefore, it is important to note that educators should not necessarily teach students what the current topics and changes are in cybersecurity. Instead, they should focus on the skills and abilities that will allow students to continually possess knowledge of current events and changes in thefield [21, 27].

The knowledge of operating systems and of logic and logic structures are endemic to most computer science education, though as CSEC2017 acknowledges, cybersecurity is a wide domain that encompasses many disciplines [45] and so curriculum developers should ensure that all students within their cybersecurity programs are exposed to these general but important topics.

At least two of the topics outlined in CSEC2017, network traffic analysis and data analytics, stress the need for students to understand packet-analysis. Our participants echoed that sentiment. Thus, cybersecurity curriculum developers should aim to include content concerning packet analysis.

4.1.2 Skills. As was the case for knowledge, it seems likely that the skills rated as relatively important are the most general and timeless. All of the soft skills cybersecurity professionals identified in previous research [46] were rated as being relatively important: skill in collaborating with the people you work with (KSA 2), skill in staying motivated (KSA 3), skill in written communication (KSA 5), skill in communication with clients or users (KSA 7), and skill in communication with management (KSA 8).

That outcome echoes the ABET engineering criteria [78] and CSEC2017 [45], which is why it is surprising tofind so few soft skills listed in the NICE Framework [29]. Those that are included in the NICE Framework (e.g., Ability to collaborate effectively with others and Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means) are not listed under the Protect and Defend specialty area. Soft skills are an expected outcome of a cybersecurity education according to both CSEC2017 and ABET [1, 45], though it is expected that such skills will be covered through general education requirements [45]. More generally, the fact that all communication skills present in this study were rated as relatively important supports previous calls for the integration of soft skills into cybersecurity education [26, 29, 40, 51].

Many have written on pedagogical techniques and on potential stumbling blocks regarding the incorporation of soft skills into the curricula for technicalfields, including computer science [11, 18], information technology [10], and engineering [78]. Students oftenfind value in soft skills [47], but do not appreciate courses dedicated to soft skills [72], which suggests that these skills should be incorporated into more technical courses. For example, students in technical courses may practice and demonstrate their communication skills through course requirements such as writing business documents or giving professional presentations [10]. Courses centered around a long-term project, such as client-sponsored project courses or capstones, provide another means of integrating soft-skills [18, 63]. Such courses and collaborative projects generally are high-impact educational practices in that they have strong effects on student engagement and success [50]. Post-graduation, soft skills play an important role in the retention of hired graduates in cybersecurity and relatedfields [4, 46]. Though this has not always been reflected in job postings and the hiring process [2], there is some indication that internationally more postings do indicate the desire that cybersecurity professionals are proficient in soft skills [67, 68]. Skills relating to teamwork are among the most common soft skill requirements found in job postings [16], suggesting that particular curricular emphasis on team projects may provide the greatest impact when graduates apply for cybersecurity jobs.

Although programming languages generally are considered highly important for cybersecurity jobs [46], the professionals we interviewed did not consider any of thefive languages we asked about to be relatively important. Python and Java (KSAs 13 and 15) were rated as neither relatively important nor relatively unimportant (neutral). C++, Ruby, and Perl (KSAs 16–19) were rated as relatively unimportant. This may indicate that while it is imperative for cyber defense professionals to know a programming language, there isflexibility as to which languages they should know. In terms of applying these results to curricular development, some research suggests Python is among the most important languages for cybersecurity professionals to know [38], and results in better course performance [83]. That said, programs may have a tendency to over-emphasize the importance of programming skills relative to industry needs as indicated by ourfindings and by a recent analysis of job ads [68].

4.1.3 Abilities. Two of the two abilities that were common to all cyber defense careers were rated as relatively important: the ability to be curious (KSA 1) and the ability to be adaptable (KSA 6). Both of those abilities are highly related to the knowledge of current events and changes in the field. As a cybersecurity professional, one must be curious to continually stay abreast of recent technological advances and willing to adapt their work to address such changes. As the CSEC2017 report acknowledges, adaptability is also important for cybersecurity professionals in that it will help them learn new technologies [45].

Curiosity, while to some extent a trait that varies between students, may be taught or at least encouraged. Indeed, many undergraduates leave school with the belief that their classes facilitated learning how to apply principles in new contexts [43]. The inquiry based method, in which students answer an initial question and use the knowledge they learn along the way to formulate subsequent questions, may both stimulate curiosity and engage those who are already curious [66, 91].

Adaptability may also be taught to some extent. Two topics outlined in CSEC2017 may encompass adaptability: behavior under uncertainty and strategic planning [45]. Curiosity and adaptability are arguably related to ones' ability to learn on one's own, which will be covered later in the discussion of CNDA KSAs.

4.2 Teaching CNDA KSAs

4.2.1 Knowledge. Fifteen of the 20 knowledge topics unique to the CNDA specialty area were rated as relatively important, and the remaining 5 knowledge topics were rated as neither relatively important nor relatively unimportant (neutral). Because none of the knowledge KSAs were rated as relatively unimportant, programs interested in specializing in CNDA should cover as many of the 20 CNDA knowledge topics as feasible.

Inspection of the 5 confidence intervals that overlapped with the importance scale's neutral point suggests some of our participants considered those knowledge topics to be relatively important. For example, the confidence interval for knowledge of cryptology (KSA 39) ranged from 3.13 to 5.60. The upper limit of that confidence interval (5.60) is equal to or greater than the upper limits of confidence intervals for other knowledge topics that were rated as relatively important. That suggests some, but not all, of our participants considered knowledge of cryptology (KSA 39) to be relatively important to their work, which suggests knowledge requirements may vary considerably from CNDA position to CNDA position.

In our opinion, such cases have two implications. First, they reinforce that programs specializing in CNDA should strive to cover as many of the related knowledge topics as feasible, even those that participants rated as neither relatively important nor unimportant (neutral). Second, such cases also reinforce the need for students to learn how to learn [44]. That way, as professionals, they can readily adapt when a new position brings with it new knowledge requirements.

Teaching students how to learn involves three main components. First, instructors ask students to answer questions and to explain the reasoning behind their answers to probe students' understanding [44]. Second, instructors, or sometimes peers, provide students feedback regarding their understanding that is not in the form of grades or other marks [17]. Third, students assess and reflect on their performance [44]. Teaching students how to learn has been highly effective [13], and may benefit students studying CNDA, in particular, because as professionals, they will likely find that knowledge requirements vary greatly from position to position.

4.2.2 Skills. One of the 12 skills unique to the CNDA specialty area was rated as relatively important: skill in collecting data from a variety of computer network defense resources (KSA 31). All other skills were rated as neither relatively important or relatively unimportant (neutral).

Inspection of the 10 confidence intervals that overlapped with the importance scale's neutral point suggests some of our participants considered those skills to be relatively important. As discussed in Section 4.2.1, in our opinion, such cases suggest programs specializing in CNDA should strive to cover as many of the related skills as possible. In addition, such programs should focus on learning how to learn, because, as professionals, their students will likelyfind that skill requirements vary greatly from position to position.

4.2.3 Abilities. One of the 1 abilities unique to the CNDA specialty area was rated as relatively important, i.e., the ability to interpret/incorporate data from multiple tools (KSA 22). Due to the complexity of this ability, there is great interest in developing data visualization tools that can help cybersecurity professionals incorporate and interpret data [33]. In the meantime, data integration is incorporated in many computer science curricula and educators are incorporating new applications of data integration into their courses [89] and exploring methods of teaching data integration to students outside of computer science and relatedfields [73].

4.3 Teaching CNDIS KSAs

4.3.1 Knowledge. One of the 6 knowledge topics unique to the CNDIS specialty area was rated as relatively important, i.e., knowledge of the types of intrusion detection software and hardware (KSA 54). Accordingly, we recommend that programs specializing in CNDIS prioritize covering that topic.

Four of the 6 knowledge topics unique to the CNDIS specialty area were rated as neither relatively important nor relatively unimportant (neutral). Inspection of those 4 confidence intervals suggests some participants considered 3 of the 4 of those knowledge topics to be relatively important: knowledge of processes for reporting network security related incidents (KSA 56), knowledge of web-filtering technologies (KSA 57), and knowledge of transmission methods (KSA 58). The exception was the confidence interval for knowledge of CMMI (KSA 60), whose upper limit (3.67) barely exceeded the importance scale's neutral point (3.5) and whose lower limit approached the lower limit (1.22) of the importance scale (1).

As discussed in Section 4.2.1, in our opinion, cases such as those for KSAs 56, 57, and 58 suggest programs specializing in CNDIS should strive to cover those knowledge topics when feasible, even though participants rated those KSAs as neither relatively important or relatively unimportant (neutral). In addition, such programs should focus on learning how to learn, because, as professionals, their students will likelyfind that knowledge requirements vary greatly from position to position.

One of the six knowledge topics unique to the CNDIS specialty area was rated as relatively unimportant, i.e., knowledge of voice-over-IP (KSA 61). Accordingly, we recommend that programs specializing in CNDIS prioritize teaching other topics over knowledge of voice-over-IP (KSA 61).

Similarly, we recommend prioritizing teaching other topics over knowledge of CMMI (KSA 60) given that many participants rated it as relatively important.

4.3.2 Skills. Two of the two skills unique to the CNDIS specialty area were rated as neither relatively important nor relatively unimportant (neutral): Skill in using VPN devices and encryption (KSA 55), and skill in tuning sensors (KSA 59). Inspection of those two confidence intervals revealed that both are quite wide. Specifically, the confidence interval for KSA 55 ranges from 2.44 to 5.28. Similarly, the confidence interval for KSA 59 ranges from 1.70 to 5.40. Intervals ranging from such low values to such high values suggests that whether these skills are important to a CNDIS professional's position varies greatly from position to position.

As discussed in Section 4.2.1, in our opinion, cases such as those for KSA 55 and KSA 59 suggest programs specializing in CNDIS should strive to cover those skills when feasible, even though participants rated those KSAs as neither relatively important nor relatively unimportant (neutral). In addition, such programs should focus on learning how to learn, because, as professionals, their students will likelyfind that skill requirements vary greatly from position to position.

4.4 Teaching VAAM KSAs

4.4.1 Knowledge. None of the KSAs unique to the VAAM specialty area were rated as being relatively unimportant. This suggests educators should generally aim to include all of those KSAs within their specialized curricula while keeping in mind that some KSAs will be more important to their students upon graduation than others will be.

Four of the seven knowledge topics unique to the VAAM specialty area were rated as being relatively important. These knowledge topics dealt with system diagnostics and vulnerabilities: knowledge of system and application security threats and vulnerabilities (KSA 68), knowledge of application vulnerabilities (KSA 71), knowledge of system diagnostic tools (KSA 72), and knowledge of network access, identity, and access management (KSA 74).

Three types of knowledge were rated as neither relatively important nor relatively unimportant (neutral): knowledge of interpreted and compiled computer languages (KSA 75), knowledge of local and specialized system requirements (KSA 77), and knowledge of relevant laws, policies, and so on, related to critical infrastructure (KSA 78). Overall, the confidence intervals for these three KSAs were not highly variable, suggesting that VAAM professionals rated the importance of these KSAs in a relatively consistent manner.

4.4.2 Skills. Two skills unique to the VAAM specialty area were rated as relatively important: skill in using penetration testing tools (KSA 70) and skill in assessing the robustness of security systems and designs (KSA 73). The remaining three VAAM skills were rated as neither relatively important nor relatively unimportant (neutral). As with the knowledge KSAs, this suggests students would benefit from the inclusion of allfive skills in their curricula but that KSAs 70 and 73 should be prioritized most highly.

4.4.3 Abilities. The one ability unique to the VAAM specialty area, the ability to identify systemic security issues based on analysis, was rated as relatively important. This suggests that this ability should be prioritized in VAAM-related curricula.

4.5 Limitations

The present results revealed many important insights. However, those insights should be considered in the context of this study's limitations, which concern how we collected our data and sample.

Regarding our data, it is important to note that the data collected for the present study are subjective ratings. As such, those ratings may not perfectly reflect how important or difficult to learn were the KSAs. For example, participants may have rated certain KSAs as relatively unimportant, because they are used relatively infrequently, despite being important during those infrequent times when those KSAs are needed. Objective ways to assess how important are KSAs to cybersecurity work were in development when the study was conducted [53] but were not available at that time. Accordingly, subjective ratings of importance and difficulty to learn were the best available option.

Regarding our sample, it is important to note that the sample size and sampling method both potentially limit our study's generalizabilty. Concerns related to sample size and sampling method will be discussed separately below.

Regarding our sample size, 48 cybersecurity professionals participated in this study, which is a relatively small sample for survey data. A larger sample would have increased the likelihood that our sample represented the population. However, it is quite difficult for researchers to collect data from cybersecurity professionals [3, 8, 15], which often prevents the collection of large samples. In the present study, we collected as much data as possible given our resources, resulting in a sample size that is consistent with or greater than those of many previous studies in which participants were cybersecurity professionals [22, 28, 30, 38, 62, 69].

On a related note, our effective sample size shrunk when we divided our participants into the four specialty areas so that we could analyze the KSAs unique to each cyber defence specialty area. Separating participants in that way would have resulted in a loss of statistical power had we employed traditional inferential statistics. To avoid that problem, we utilized bootstrapping to estimate population parameters. With that said, the results of bootstrapping may not accurately reflect population parameters if the initial sample does not reflect the variability found in the broader population, and it is not appropriate for sample sizes of 8 or smaller [6, 7, 31, 61]. For the most part, sample sizes for each specialty area exceeded that criterion, the exceptions being difficulty to learn ratings for the CNDIS specialty area and importance and difficulty to learn ratings for the IR specialty area. Regarding the former, despite having 10 participants who affiliated with the CNDIS specialty area, response rates for some difficulty to learn ratings were low enough that the results of the bootstrapping should be interpreted with caution. Regarding the latter, only four participants identified as being affiliated with the IR specialty area. Accordingly, we did not conduct bootstrapping on those participants' data, and instead presented raw descriptive statistics for that group. Those descriptive statistics should be interpreted with caution given that small number of participants associated with that speciality area.

Regarding our sampling method, participants in the current study attended one of two hacking conferences held in the United States, Black Hat and DEF CON. We collected data at these venues, because it was our understanding that cybersecurity professionals would be suspicious of electronic data collection [8], e.g., they might perceive a request to complete an electronic survey or an over-the-phone survey to be a social engineering attack. Accordingly, we deemed it necessary to conduct data collection face-to-face and via non-electronic means. To do so, we decided to collect data at Black Hat and DEF CON, because they are premiere cybersecurity conferences that draw large and diverse groups of cybersecurity professionals. In 2017, over 17,000 people attended Black Hat [14] and 25,000 people attended DEF CON [84]. Nevertheless, our sample is a convenience sample, like many others concerning cybersecurity experts [9, 35, 80]. Accordingly, the nature of our sample could potentially limit our results' generalizability if Black Hat and DEF CON attendees are somehow different than the average cybersecurity professional. Unfortunately, Black Hat and DEF CON do not provide information regarding attendees out of concern that someone might try to use that information for nefarious purposes. Therefore, we cannot directly speak

to whether Black Hat and DEF CON attendees truly represent the average cybersecurity professional; although, we have no reason to suspect that they do not. With that said, we do take solace in the fact that our data regarding participants' educational backgrounds and their time spent working in cybersecurity are consistent with those from previous studies [35, 74].

4.6 Conclusions

Ourfindings provide important information that educators can use when designing curricula related to the CNDA, CNDIS, and VAAM specialty area. For example, educators can prioritize KSAs based on rated importance, with KSAs rated as relatively important being prioritized the highest.

With that said, it is important to note that cybersecurity is a rapidly evolvingfield [21, 27, 29], and ourfindings provide a snapshot at one point in time. However, we think some of the individual KSAs rated as being highly important, such as those common across all cyber defense specialty areas, may withstand the test of time. Many of the common KSAs rated as being highly important stressed adaptability and continued learning post-graduation (KSAs 1, 3, 4, and 6). The necessity of continued learning was echoed when examining the ratings of KSAs unique to each specialty group. For example, particularly within the CNDA and CNDIS specialty areas, our results revealed that importance ratings for certain knowledge and skills were highly variable, which suggests knowledge and skill requirements vary considerably between positions. In such cases, adaptability and knowing how to learn will be critical.

Unfortunately, only a few our participants reported being employed within IR, and as a result we did not collect enough information to infer the importance of KSAs within the IR specialty area. It would be beneficial for future research to investigate the relative importance of the KSAs within IR. This is especially true given that intrusion detection, a key component of IR, may require a relatively unique skill set compared to other cyber domains [38].

Continued research will be necessary to stay abreast of the new or newly important KSAs relevant to cyber work. Additionally or alternatively to future research, cybersecurity programs may wish to form direct industry connections. Such connections and subsequent redesign of courses and curricula due to industry input can pose challenges [55] but also result in bene fi ts to the program [87], students [86], and faculty research [85]. In addition to informing educators about what KSAs are in demand at that time, such partnerships may also result in increased graduate employment and in said graduates later instrumenting the funding for program developments [86].

In sum, we intend for our research to serve as a means for educators to make informed decisions about specialized cybersecurity curricula. Additionally, we present some suggestions on how to interpret the KSA ratings and on pedagogical tools that may prove useful when implementing our findings.

ACKNOWLEDGMENT

The authors thank Max Ogunfunwa for his assistance with data collection.

REFERENCES

[1] 2018. ABET Approves Accreditation Criteria for Undergraduate Cybersecurity Programs. Retrieved from https://www.abet.org/abet-approves-accreditation-criteria-for-undergraduate-cybersecurity-programs/.

[2] Cheryl L. Aasheim and Susan R. Williams. 2009. Knowledge and skill requirements for entry level information technology workers: Do employers in the IT industry vie these differently than employers in other industries. Retrieved from https://digitalcommons.georgiasouthern.edu/information-tech-facpubs/.

[3] Robert G. Abbott, Jonathan McClain, Benjamin Anderson, Kevin Nauer, Austin Silva, and Chris Forsythe. 2015. Log analysis of cyber security training exercises. *Proc. Manufact.* 3 (2015), 5088–5094.

[4] Thomas Abraham, Cynthia Beath, Christine Bullen, Kevin Gallagher, Tim Goles, Kate Kaiser, and Judith Simon. 2006. IT workforce trends: Implications for IS programs. *Commun. Assoc. Inf. Syst.* 17, 1 (2006), 1147–1170.

[5] Ralitsa B. Akins, Homer Tolson, and Bryan R. Cole. 2005. Stability of response characteristics of a Delphi panel: application of bootstrap data expansion. *BMC Med. Res. Methodol.* 5, 1 (2005), 37.
[6] Todd R. Andel and J. Todd McDonald. 2013. A systems approach to cyber assurance education. In *Proceedings of the Information Security Curriculum Development Conference (InfoSecCD'13)*. ACM, 13.
[7] Handan Ankarali, Ayşe Canan Yazici, and Seyit Ankarali. 2009. A bootstrap confidence interval for skewness and kurtosis and properties of t-test in small samples from normal distribution.*Med. J. Trakya Univ.* 26, 4 (2009).
[8] Miriam E. Armstrong, Keith S. Jones, and Akbar Siami Namin. 2017. Framework for developing a brief interview to understand cyber defense work: An experience report. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 61. SAGE, Los Angeles, CA, 1318–1322.
[9] Masooda Bashir, Colin Wee, Nasir Memon, and Boyi Guo. 2017. Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Comput. Secur.* 65 (2017), 153–165.
[10] Debbie Beard, Dana Schweiger, and Ken Surendran. 2019. Integrating soft skills assessment through university, college, and programmatic efforts at an AACSB accredited institution. *J. Inf. Syst. Educ.* 19, 2 (2019), 11.
[11] Aseel Berglund and Fredrik Heintz. 2014. Integrating soft skills into engineering education for increased student throughput and more professional engineers. In *Proceedings of LTHs 8: e Pedagogiska Inspirationskonferens (PIK'14)* (2014), 1–3.
[12] Ali Bicak, Xiang Michelle Liu, and Diane Murphy. 2015. Cybersecurity curriculum development: Introducing specialties in a graduate program. *Inf. Syst. Educ. J.* 13, 3 (2015), 99.
[13] Paul Black and Dylan Wiliam. 1998. Assessment and classroom learning. *Assess. Educ.: Principles Pol. Pract.* 5, 1 (1998), 7–74.
[14] Black Hat. 2017. Black Hat celebrates 20 years with record breaking USA event. Retrieved from https://www.prnewswire.com/news-releases/black-hat-celebrates-20-years-with-record-breaking-usa-event-300496433.html.
[15] Brett Borghetti, Gregory Funke, Robert Pastel, and Robert Gutzwiller. 2017. Cyber Human research from the cyber operator's view. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 61. SAGE, Los Angeles, CA, 350–350.
[16] Nita G. Brooks, Timothy H. Greer, and Steven A. Morris. 2018. Information systems security job advertisement analysis: Skills review and implications for information systems curriculum. *J. Educ. Bus.* 93, 5 (2018), 213–221.
[17] Ruth Butler. 1988. Enhancing and undermining intrinsic motivation: The effects of task-involving and ego-involving evaluation on interest and performance. *Br. J. Educ. Psychol.* 58, 1 (1988), 1–14.
[18] Lori Carter. 2011. Ideas for adding soft skills education to service learning and capstone courses for computer science students. In *Proceedings of the 42nd ACM Technical Symposium on Computer Science Education*. 517–522.
[19] Phil Casesa. 2018. The 5 most in-demand cyber security jobs for 2019. Retrieved from https://blog.focal-point.com/the-5-most-in-demand-cyber-security-jobs-2019.
[20] Center for Strategic and International Studies. 2016. Hacking the skills shortage: A study of the international shortage in cybersecurity skills.Retrieved November 30, 2018 from https://www.mcafee.com/fr/resources/reports/rp-hacking-skills-shortage.pdf.
[21] Michael Champion, Shree Jariwala, Paul Ward, and Nancy J. Cooke. 2014. Using cognitive task analysis to investigate the contribution of informal education to developing cyber security expertise. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 58. SAGE, Los Angeles, CA, 310–314.
[22] Michael A. Champion, Prashanth Rajivan, Nancy J. Cooke, and Shree Jariwala. 2012. Team-based cyber defense analysis. In *Proceedings of the 2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*. IEEE, 218–221.
[23] Tamara Chuang. 2018. Ransomware strikes CDOT for second time even as agency still recovering fromfirst SamSam attack. *The Denver Post* (March 2018). Retrieved from https://www.denverpost.com/2018/03/01/cdot-samsam-ransomware-attack/.
[24] Stephen Cobb. 2016. Mind this Gap: Criminal hacking and the global cybersecurity skills shortage, a critical analysis. In *Proceedings of the Virus Bulletin Conference*. 1–8.
[25] Art Conklin. 2006. Cyber defense competitions and information security education: An active learning solution for a capstone course. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, Vol. 9. IEEE, 220b–220b.
[26] Wm Arthur Conklin, Raymond E. Cline, and Tiffany Roosa. 2014. Re-engineering cybersecurity education in the US: an analysis of the critical factors. In *Proceedings of the 2014 47th Hawaii International Conference on System Sciences*. IEEE, 2006–2014.
[27] Michael Cook. 2014. *Cyber Acquisition Professionals Need Expertise (But They Don't Necessarily Need to Be Experts)*. Technical Report. Defense Acquisition University.

[28] Jennifer Cowley. 2014. *Job Analysis Results for Malicious-code Reverse Engineers: A Case Study*. Technical Report. Carnegie-Mellon University Software Engineering Institute.
[29] Jessica Dawson and Robert Thomson. 2018. The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Front. Psychol.* 9 (2018).
[30] Anita D'Amico and Kirsten Whitley. 2008. The real work of computer network defense analysts. In *Proceedings of the VizSEC 2007*. Springer, 19–37.
[31] B. Efron. 1995. Computers, bootstraps, and statistics. In *Invited Address to American Educational Research Association Annual Meeting, Division D–Measurement and Research Methodology*.
[32] Steve Evans. 2016. Data Breach Costs Soaring. Retrieved from https://www.infosecurity-magazine.com/news/data-breach-costs-soaring/.
[33] Glenn A. Fink, Christopher L. North, Alex Endert, and Stuart Rose. 2009. Visualizing cyber security: Usable workspaces. In *Proceedings of the 2009 6th International Workshop on Visualization for Cyber Security*. IEEE, 45–56.
[34] Jennifer Fowler and Nate Evans. 2019. Using the NICE framework as a metric to analyze student competencies. In *Proceedings of The Colloquium for Information System Security Education (CISSE)*.
[35] Sarah E. Freed. 2014. *Examination of Personality Characteristics Among Cybersecurity and Information Technology Professionals*. Ph.D. Dissertation. University of Tennessee at Chattanooga. https://scholar.utc.edu/theses/127/.
[36] Frost & Sullivan. 2017. 2017 Global Information Security Workforce Study: Benchmarking workforce capacity and response to cyber risk. Retrieved October 16, 2019 from https://iamcybersafe.org/gisws.
[37] Ken Goldman, Paul Gross, Cinda Heeren, Geoffrey L. Herman, Lisa Kaczmarczyk, Michael C. Loui, and Craig Zilles. 2010. Setting the scope of concept inventories for introductory computing subjects. *ACM Trans. Comput. Educ.* 10, 2 (2010), 1–29.
[38] John R. Goodall, Wayne G. Lutters, and Anita Komlodi. 2009. Developing expertise for network intrusion detection. *Inf. Technol. People* 22, 2 (2009), 92–108.
[39] Julie M. Haney and Wayne G. Lutters. 2017. Skills and characteristics of successful cybersecurity advocates. In *Proceedings of the Workshop on Security Information Workers, Symposium on Usable Privacy and Security (SOUPS'17)*.
[40] Regina Hartley, Dawn Medlin, and Zach Houlik. 2017. Ethical hacking: Educating future cybersecurity professionals. In *Proceedings of the EDSIG Conference*, Vol. 2473. 3857.
[41] Adam P. Henry. 2017. *Mastering the Cyber Security Skills Crisis: Realigning Educational Outcomes to Industry Requirements*. Technical Report. ACCS Discussion paper.
[42] Lance Hoffman, Diana Burley, and Costis Toregas. 2011. Holistically building the cybersecurity workforce. *IEEE Secur. Priv.* 10, 2 (2011), 33–39.
[43] Denise Jackson. 2016. Skill mastery and the formation of graduate identity in bachelor graduates: Evidence from australia. *Stud. High. Educ.* 41, 7 (2016), 1313–1332.
[44] Mary James, Paul Black, Patrick Carmichael, Colin Conner, Peter Dudley, Alison Fox, David Frost, Leslie Honour, John MacBeath, Bethan Marshall, et al. 2006. *Learning How to Learn: Tools for Schools*. Routledge.
[45] Joint Task Force on Cybersecurity Education. 2017. *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. Technical Report. ACM, IEE-CS, AIS SIGSEC, IFIP WG 11.8.
[46] Keith S. Jones, Akbar Siami Namin, and Miriam E. Armstrong. 2018. The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. *ACM Trans. Comput. Educ.* 18, 3 (2018), 1–12.
[47] Sonja Kabicher, Renate Motschnig-Pitrik, and Kathrin Figl. 2009. What competences do employers, staffand students expect from a computer science graduate? In *Proceedings of the 2009 39th IEEE Frontiers in Education Conference*. IEEE, 1–6.
[48] David J. Kay, Terry J. Pudas, and Brett Young. 2012. *Preparing the Pipeline: The US Cyber Workforce for the Future (Defense Horizons, Number 72)*. Technical Report. National Defense University, Institute for National Strategic Studies.
[49] Kenneth J. Knapp, Christopher Maurer, and Miloslava Plachkinova. 2017. Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance. *J. Inf. Syst. Educ.* 28, 2 (2017), 101–114.
[50] George D. Kuh. 2008. *High-Impact Educational Practices: What They Are, Who Has Access to Them, and Why They Matter*. Association of American Colleges and Universities, Washington, D.C., 34.
[51] Jane LeClair, Sherly Abraham, and Lifang Shih. 2013. An interdisciplinary approach to educating an effective cyber security workforce. In *Proceedings of the Information Security Curriculum Development Conference (InfoSecCD'13)*. ACM, 71–78.
[52] M. Locasto and Sara Sinclair. 2009. An experience report on undergraduate cyber-security education and outreach. In *Proceedings of the Annual Conference on Education in Information Security (ACEIS'09)*.
[53] Vincent F. Mancuso, James C. Christensen, Jennifer Cowley, Victor Finomore, Cleotide Gonzalez, and Benjamin Knott. 2014. Human factors in cyber warfare II: Emerging perspectives. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 58. 415–418.

[54] Andrew McGettrick. 2013. Toward effective cybersecurity education. *IEEE Secur. Priv.* 11, 6 (2013), 66–68.
[55] Ana M. Moreno, Maria-Isabel Sanchez-Segura, Fuensanta Medina-Dominguez, and Laura Carvajal. 2012. Balancing software engineering education and industrial needs. *J. Syst. Softw.* 85, 7 (2012), 1607–1620.
[56] Dan Munro. 2016. Data breaches In healthcare totaled over 112 million records in 2015. Retrieved from https://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/b0e6e937b07f.
[57] Michael Nadeau. 2017. Cyber security jobs: Job descriptions, requirements and salaries for today's hottest roles. Retrieved from https://www.csoonline.com/article/3214480/cyber-security-jobs-job-descriptions-requirements-and-salaries-for-todays-hottest-roles.html.
[58] National Security Administration. [n.d.]. National Centers of Academic Excellence. Retrieved November 19, 2019 from https://www.nsa.gov/resources/students-educators/centers-academic-excellence/.
[59] William Newhouse, Stephanie Keith, Benjamin Scribner, and Greg Witte. 2017. *National Initiative for Cybersecurity Eduction (NICE) Cybersecurity Workforce Framework*. Technical Report. https://doi.org/10.6028/NIST.SP.800-181
[60] BBC News. 2011. UK beefs up cyber warfare plans. Retrieved from https://www.bbc.com/news/technology-13599916.
[61] Desmond C. Ong. 2014. A primer to bootstrapping; and an overview of doBootstrap. Retrieved from https://web.Stanford.edu/class/psych252/tutorials/doBootstrapPrimer.pdf.
[62] Geet Parekh, David DeLatte, Geoffrey L. Herman, Linda Oliva, Dhananjay Phatak, Travis Scheponik, and Alan T. Sherman. 2017. Identifying core concepts of cybersecurity: Results of two delphi processes. *IEEE Trans. Educ.* 61, 1 (2017), 11–20.
[63] Robert Pastel, Marika Seigel, Wei Zhang, and Alex Mayer. 2015. Team building in multidisciplinary client-sponsored project courses. *ACM Trans. Comput. Educ.* 15, 4 (2015), 1–23.
[64] Wayne Patterson, Cynthia Winston, and Lorraine Fleming. 2016. Behavioral cybersecurity: Human factors in the cybersecurity curriculum. In *Advances in Human Factors in Cybersecurity*. Springer, 253–266.
[65] Nicole Perlroth. 2017. Hackers are targeting nuclear facilities, homeland security dept. and F.B.I. say. *New York Times* (July 2017). Retrieved from https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html.
[66] Graham Pluck and H. L. Johnson. 2011. Stimulating curiosity to enhance learning. *GESJ: Educ. Sci. Psychol.* 2 (2011).
[67] Leigh Ellen Potter and Gregory Vickers. 2015. What skills do you need to work in cyber security? A look at the Australian market. In *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*. 67–72.
[68] Ibrahim Rahhal, Ibtissam Makdoun, Ghita Mezzour, Imane Khaouja, Kathleen Carley, and Ismail Kassou. 2019. Analyzing cybersecurity job market needs in morocco by mining job ads. In *Proceedings of the 2019 IEEE Global Engineering Education Conference (EDUCON'19)*. 535–543.
[69] Awais Rashid, George Danezis, Howard Chivers, Emil Lupu, Andrew Martin, Makayla Lewis, and Claudia Peersman. 2018. Scoping the cyber security body of knowledge. *IEEE Secur. Priv.* 16, 3 (2018), 96–102.
[70] Dale C. Rowe, Barry M. Lunt, and Joseph J. Ekstrom. 2011. The role of cyber-security in information technology education. In *Proceedings of the 2011 Conference on Information Technology Education*. 113–122.
[71] Henrique Santos, Teresa Pereira, and Isabel Mendes. 2017. Challenges and reflections in designing cyber security curriculum. In *Proceedings of the 2017 IEEE World Engineering Education Conference (EDUNINE'17)*. IEEE, 47–51.
[72] Mariecke Schipper and Esther van der Stappen. 2018. Motivation and attitude of computer engineering students toward soft skills. In *Proceedings of the 2018 IEEE Global Engineering Education Conference (EDUCON'18)*. IEEE, 217–222.
[73] Maria Victoria Schneider and Rafael C. Jimenez. 2012. Teaching the fundamentals of biological data integration using classroom games. *PLoS Comput. Biol.* 8, 12 (2012).
[74] David Schuster and Steven Wu. 2018. Toward cyber workforce development: An exploratory survey of information security professionals. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 62. SAGE, Los Angeles, CA, 1242–1246.
[75] Joanne Sexton, Karen Ribble, and Franklin Perrin. 2019. Addressing the cybersecurity workforce development problem—Augusta university's contribution. In *Proceedings of the Colloquium for Information System Security Education (CISSE'19)*.
[76] Tasnim Shamma. 2018. Atlanta paralyzed for more than a week by cyber attack. *National Public Radio* (March 2018). Retrieved from https://www.npr.org/2018/03/30/598386485/atlanta-paralyzed-for-more-than-a-week-by-cyber-attack.
[77] Dan Shoemaker, Anne Kohnke, and Ken Sigler. 2018. *A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)*. Auerbach Publications.
[78] Larry J. Shuman, Mary Besterfield-Sacre, and Jack McGourty. 2005. The ABET "professional skills"—Can they be taught? Can they be assessed? *J. Eng. Educ.* 94, 1 (2005), 41–55.
[79] Timothy Summers, Kalle J. Lyytinen, Tony Lingham, and Eugene A. Pierce. 2013. How hackers think: A study of cybersecurity experts and their mental models. In *Proceedings of the 3rd Annual International Conference on Engaged Management Scholarship*.

[80] 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 (2014), 53–56.
[81] UPI. 2016. Wanted: Students to enter cybersecurityfield. Retrieved from https://www.upi.com/BusinessNews/2016/08/19/Wanted-Students-to-enter-cybersecurity-field/1501471626441/.
[82] Alex Vieane, Gregory Funke, Robert Gutzwiller, Vincent Mancuso, Ben Sawyer, and Christopher Wickens. 2016. Addressing human factors gaps in cyber defense. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 60. 770–773.
[83] Jacques Wainer and Eduardo C. Xavier. 2018. A controlled experiment on python vs c for an introductory programming course: Students' outcomes. *ACM Trans. Comput. Educ.* 18, 3 (2018), 12.
[84] Wikipedia. [n.d.]. DEF CON. Retrieved from https://en.wikipedia.org/wiki/DEFCON.
[85] Claes Wohlin, Aybuke Aurum, Lefteris Angelis, Laura Phillips, Yvonne Dittrich, Tony Gorschek, Hakan Grahn, Kennet Henningsson, Simon Kagstrom, Graham Low, et al. 2011. The success factors powering industry-academia collaboration. *IEEE Softw.* 29, 2 (2011), 67–73.
[86] Belle Woodward, Thomas Imboden, and Nancy L. Martin. 2013. An undergraduate information security program: More than a curriculum. *J. Inf. Syst. Educ.* 24, 1 (2013), 63.
[87] Belle S. Woodward and Travis Young. 2007. Redesigning an information system security curriculum through application of traditional pedagogy and modern business trends. *Inf. Syst. Educ. J.* 5, 11 (2007), 1–11.
[88] Muhammad Mudassar Yamin and Basel Katt. 2019. Cyber security skill set analysis for common curricula development. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*. 1–8.
[89] Li Yang and Xumin Liu. 2013. Teaching business analytics. In *Proceedings of the 2013 IEEE Frontiers in Education Conference (FIE'13)*. IEEE, 1516–1518.
[90] Weimo Zhu. 1997. Making bootstrap statistical inferences: A tutorial. *Res. Quart. Exercise Sport* 68, 1 (1997), 44–55.
[91] Michal Zion and Irit Sadeh. 2007. Curiosity and open inquiry learning. *J. Biol. Educ.* 41, 4 (2007), 162–169.

Received February 2019; revised June 2020; accepted July 2020