How do Computing Students Conceptualize Cybersecurity? Survey Results and Strategies for Curricular Integration

Noah Q. Cowit
Department of Information Science
University of Colorado Boulder
Boulder, CO, USA
Noah.Cowit@colorado.edu

Vidushi Ojha
Department of Computer Science
University of Illinois at Urbana-Champaign
Urbana-Champaign, IL, USA
vojha3@illinois.edu

Casey Fiesler
Department of Information Science
University of Colorado Boulder
Boulder, CO, USA
Casey.Fieslser@colorado.edu

ABSTRACT

Cybersecurity expertise continues to be relevant as a means to confront threats and maintain vital infrastructure in our increasingly digitized world. Public and private initiatives have prioritized building a robust and qualified cybersecurity workforce, requiring student buy-in. However, cybersecurity education typically remains siloed even within computer and information technology (CIT) curriculum. This paper's goal is to support endeavors and strategies of outreach to encourage interest in cybersecurity. To this end, we conducted a survey of 126 CIT students to investigate student perceptions of cybersecurity and its major crosscutting concepts (CCs). The survey also investigates the prevalence of preconceptions of cybersecurity that may encourage or dissuade participation of people from groups underrepresented in computing. Regardless of prior learning, we found that students perceive cybersecurity as a relatively important topic in CIT. We found student perspectives on conceptual foundations of cybersecurity were significantly different ($p<.05$) than when simply asked about "cybersecurity," indicating many students don't have an accurate internal construct of the field. Several previously studied preconceptions of cybersecurity were reported by participants, with one misconception — that cybersecurity "requires advanced math skills" — significantly more prevalent in women than men ($p< .05$). Based on our findings, we recommend promoting cybersecurity among post-secondary students by incorporating elements of cybersecurity into non-cybersecurity CIT courses, informed by pedagogical strategies previously used for other topics in responsible computing.

CCS CONCEPTS

• Social and professional topics • Computer science education • Security and privacy

KEYWORDS:

Cybersecurity, Curriculum Design Recommendations, Survey Results, Responsible Computing, Secure Computing

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

ACM ISBN 979-8-4007-0423-9/24/03. https://doi.org/10.1145/3626252.3630869

ACM Reference format:

Noah Q. Cowit, Vidushi Ojha, and Casey Fiesler. 2023. How do Computing Students Conceptualize Cybersecurity? Survey Results and Strategies for Curricular Integration. In *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE 2024),* March 20--23, 2024, Portland, OR, USA. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3626252.3630869

1 INTRODUCTION

The relevance of cybersecurity expertise (e.g., in adversarial thinking and risk assessment/management) has never been more clear, both with respect to securing new technologies and protecting older ones (e.g., public infrastructure). Though knowledge of cybersecurity is critical for specialists, it is also relevant across a wide range of computer and information technology (CIT) topics, since lack of knowledge in fundamental cybersecurity concepts among CIT professionals can introduce vulnerabilities in essential digital infrastructure. However, within CIT, cybersecurity courses are typically upper division electives—if they are offered at all—which means that it is possible if not likely that undergraduate CIT students will not learn about the topic [6, 42]. In graduate education, students pursuing a master's degree in CIT with an emphasis in a non-cybersecurity topic are likely to not even have a course available to them in cybersecurity, despite potential interest or relevance.

Therefore, incoming post-secondary students who are interested in CIT often must make decisions about whether to pursue optional cybersecurity courses based on previously existing biases and preconceptions about the topic, as well as underdeveloped conceptual understandings of what coursework and careers in cybersecurity entail. If student preconceptions of this topic do not line up with students' understandings of important or useful knowledge in CIT, their own self-efficacy, and/or desire for belonging, students may not choose to take courses in cybersecurity, depriving the field of valuable contributors, students of potentially enriching careers, and the public of safe and dependable CIT systems.

The study presented here investigates students' perceptions of cybersecurity. Thus, we ask the following research questions:

1. To what degree do students believe learning about cybersecurity is important to becoming a CIT professional?

2. To what degree is interest in cybersecurity different between students who have taken cybersecurity courses and those who haven't?
3. To what degree do students consider crosscutting concepts (CCs) of cybersecurity important for learning about and working in CIT, individually and when compared with cybersecurity in general?
4. To what degree do students believe preconceptions of cybersecurity that may dissuade or encourage participation of people from groups underrepresented in computing?

For each research question, we also investigated to what degree group differences (e.g., gender) influenced respondents' results.

To answer these questions, we conducted a survey of 126 students at the University of Colorado Boulder — a large public research university in the United States — using descriptive statistics and hypothesis tests to answer our research questions. We found that students consider cybersecurity to be important, regardless of prior experience. Students reported CCs to be significantly more important than cybersecurity, pointing to a lack of conceptual understanding of the subject. We also identified several previously studied preconceptions of cybersecurity in our sample, with one misconception more prevalent among women ("requires advanced math"). Finally, we recommend strategies of cybersecurity outreach and integration, motivated by our findings and strategies previously used in other topics in responsible computing.

2 BACKGROUND AND MOTIVATION

Cyberthreats are a real and growing problem to our societal infrastructure, with profound negative impacts to economic output, the information space, and personal privacy [10, 15, 19, 25, 27, 38]. This has encouraged large, public secure computing initiatives in the USA and Europe [32, 37]. "Cybersecurity" education has also been a recent topic of interest within the ACM research community, with a 2020 literature review finding 71 relevant papers published in SIGCSE and ITICSE from 2010 to 2019 [35]. This is apt, as the development of a well-qualified cybersecurity workforce must start with student buy-in. While research has been conducted measuring student attitudes towards CIT (and has consistently found a gender gap between men and women) [2, 39, 40], it is also important to understand to what degree cybersecurity is considered important by post-secondary CIT students as a subtopic within the larger field.

In 2017, a Joint Task Force (JTF) of computing professional organizations ACM, IEEE, AIS SIGSEC, and IFIP released global guidelines on cybersecurity curricula composed of both conceptual knowledge and practical skill to create "the leading resource of comprehensive cybersecurity curricular content for global academic institutions seeking to develop a broad range of cybersecurity offerings at the post-secondary level" [20]. These guidelines are based on previously existing curricular recommendations along with new developments and have since been adopted as the standard for cybersecurity accreditation by ABET, the preeminent post-secondary accreditation organization of CIT programs in the USA, the country from which our sample was drawn [31, 46]. They are designed to be interdisciplinary, to mirror the nature of cybersecurity in the contemporary world [9]. To this end, the guidelines name six crosscutting concepts (CCs) which make up the basic foundation of the study and practice of cybersecurity [3, 20]: *Confidentiality: "*Rules that limit access to system data and information to authorized persons"; *Integrity:* "Assurance that the data and information are accurate and trustworthy"; *Availability: "*The data, information, and system are accessible"; *Risk:* "Potential for gain or loss"; *Adversarial Thinking:* "A thinking process that considers the potential actions of the opposing force working against the desired result"; *Systems Thinking:* "A thinking process that considers the interplay between social and technical constraints to enable assured operations".

These CCs are prevalent among the national and international cybersecurity higher education community, and accepted as a framework for teaching and accreditation [18, 46]. In addition to their theoretical relevance to cybersecurity, it is reasonable to assume the six CCs are representative in understanding how cybersecurity as a discipline is conceptualized and taught in post-secondary education in the USA. It is unclear, however, whether post-secondary students with and without cybersecurity experience also conceptualize the discipline through these CCs. For instance, an incoming student may think cybersecurity is very important to becoming a CIT professional but believe none of the CCs are important to the same goal, or vice versa. Probing student understanding of the CCs is a precise way of ensuring valid constructs when asking questions about cybersecurity. In addition, by understanding students' perspectives on the usefulness of these CCs and comparing them to their perspectives of cybersecurity as a whole, we can gain insight as to the accuracy of students' perceptions of what work in the discipline conceptually entails. This is important to quantify, as a lack of clarity about cybersecurity can allow the development of potentially harmful misconceptions.

Prior work has found that students tend to have pre-existing conceptions about cybersecurity even if they have yet to take a course in the subject. In a study by Ojha et al., the authors interviewed undergraduate CS majors about their perceptions of cybersecurity and found that students had specific beliefs regarding the types of people who are in cybersecurity, the kind of work they do, and the social impact of this work [30]. In particular, they found that students believed cybersecurity is a challenging field and that it is largely for men. Students reported believing that cybersecurity has the potential to impact society, albeit not always in good ways, with students citing stereotypes about "hackers". These findings align with documented stereotypes about the field of computing more broadly; that it requires brilliance [23], is largely the domain of men [5], and may not positively impact society [11]. Preconceptions such as these may differentially impact women and students from historically underrepresented groups in CIT, which may affect efforts to broaden participation in computing and in cybersecurity [30]. As curricular recommendations for post-secondary CIT programs are reworked [47], understanding the student conception of

cybersecurity is valuable both in understanding how current practices impress upon students different topics in CIT, and in developing strategies of encouraging student interest and participation.

3 METHODS

To conduct this research, we fielded an anonymous survey to undergraduate students enrolled in CIT courses at a large, public US university in May and June 2023 using Qualtrics software. This study was approved by a university IRB, and no financial or academic incentive was offered for participation.

Survey Items. The survey questions can be divided into four categories, described below, plus participant information/demographics. Survey items included either a Likert scale ("To what extent to you agree or disagree with the following statement") or nominal choices, with a "don't know" option that was placed outside of the scale to minimize the ambiguity of midpoints [29]. Following best practices to avoid question ordering effects, questions are presented from most general to most specific [12]. Survey items included:

CIT Topic Importance: Participants were prompted to choose three most and least important CIT subject areas, using the ACM computing classification system as a basis [8]. This was slightly modified to increase accessibility to participants and to improve construct validity ("security and privacy" -> "cybersecurity").

General Cybersecurity: Participants reported to what extent they "expect computer and information technology programs to teach about cybersecurity", consider cybersecurity "important to securing a job" in CIT, and "expect to use cybersecurity throughout a career" in CIT. Participants were also asked whether they had previously learned about cybersecurity in their coursework.

Preconceptions of Cybersecurity: The interview results found by Ojha et al. [30] were operationalized into questions for this survey (e.g., "Cybersecurity requires advanced math skills").

Crosscutting Concepts of Cybersecurity: CCs were each defined for participants per best practices in survey design [12]. The questions about each CC were identical to the general cybersecurity questions, except participants also reported to what degree they thought each concept applied to cybersecurity.

Participant Information / Demographics: Participants reported relevant information to the survey (e.g., year in school) as well as demographic categories (e.g., race, gender).

Sample Development. Participants were recruited from the University of Colorado Boulder. All instructors teaching a computer or information science class were contacted in Spring 2023 with an email prompt explaining this research and asking them to share the survey with their students.

Sample Profile. 126 CIT students responded to the survey, with 81 participants completing the survey in its entirety and 45 partially completing the survey. Thus, the number of responses presented in the results will vary. At the beginning of the survey, participants were asked if they were "a current or prospective major or minor in Information Science, Computer Science, or another field which makes use of computer and information technologies?" Students who answered no to this question were disallowed from taking the survey. Only students who answered affirmatively proceeded to the rest of the survey.

Previous Experience in Cybersecurity: 26% of participants reported currently taking or having taken a "course covering cybersecurity topics", while 74% did not. This question was asked before the CCs were described to participants, capturing students' preconceptions of "cybersecurity topics".

Majors of Participants: Nearly all participants were computer science (49.6%) or information science majors (42.1%), with a small number of computational math/physics (3%) and engineering majors (5.3%).

Participants' Courses: Our participants were sampled from 24 information science and computer science courses. Our sample skewed towards advanced courses (56%), with participants sampled from intermediate courses (28%), and introductory courses (16%), making up comparatively less of the sample.

Year in School: 6.3% participants reported being a first year, 11.3% sophomore, 26.3% Junior, 31.3% Senior, 10% 5th/6th year undergraduate, and 10% graduate students.

Race: For participants who reported race, 72.5% reported being white, 10% South Asian / Indian, 8.8% Hispanic/Latino, 7.5% East Asian, 5% Black, 2.5% Prefer not to answer, 1.3% American Indian, and 1.3% Not listed.

Gender: For participants who reported gender, 67.1% reported as men, 30.4% reported as women, 2.5% preferred not to answer, and zero reported as non-binary/gender queer. A larger proportion of women responded to this survey (30.4%) than the national average in CIT majors (18-22%) [4, 36, 43].

Analysis. We used hypothesis testing to compare group differences, investigating group perceptions of the importance of cybersecurity, importance of CCs, and preconceptions about the field. Significant differences were found related to prior experience in cybersecurity (Chi-Squared Test [28]) and gender (Fisher's Exact Test [44]) with p-values and effect sizes (Cramer's-V [45]) noted. The sample for this survey was too small to allow for effect comparisons of racial groups underrepresented in computing. We found no notable results related to major or level of schooling, thus those relations are not discussed in the result section. Finally, we used paired t-tests to compare average total student perspectives of cybersecurity's importance to those of the CCs (and CCs to each other), with p-values and effect sizes (Cohen's-D [26]) displayed.

Limitations. It is important to note that this research is preliminary, and findings in this study need to be interpreted with a degree of caution consummate with their sample size. This is a descriptive/correlational study, preventing causal conclusions. Since decisions to share the survey were made by instructors, we cannot determine a response rate, and the sample was not random. Students who felt more warmth towards instructors may have been more likely to take this survey. The sample was not diverse in all potentially relevant dimensions (i.e., race/ethnicity). Additionally, as the sample was taken from a single university it may not be generalizable to other institutional contexts, particularly those with different student demographics or CIT curricular standards.

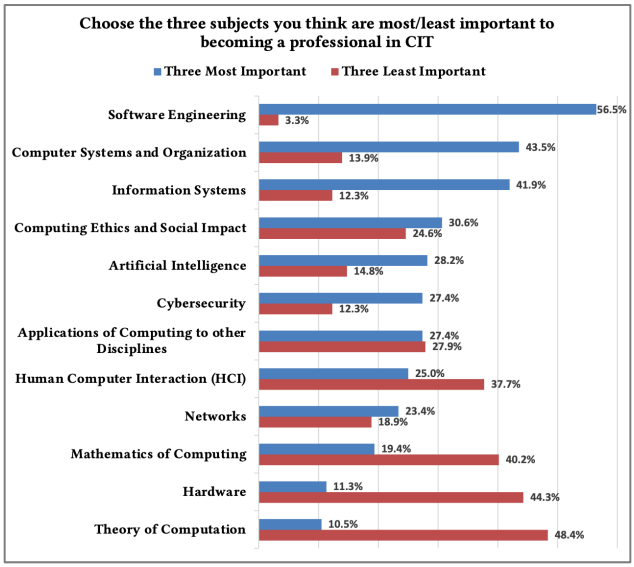
4 RESULTS

The tables based on Likert scale questions (all except 1a) correspond to ordinal 4-point scales coded from 1-Strongly Disagree to 4-Strongly Agree. Means ($\bar{x}$), standard deviations (σ) and number of responses (N) are included for all scale items. To show distribution, we include sparklines (small column charts).

4.1 Students Consider Cybersecurity an Important Topic, Irrespective of Prior Experience

With respect to CIT topic importance, as displayed in figure 1, 27.7% of participants report cybersecurity as a top three *most* important subject (6th out of the 12 subjects surveyed) when compared to other CIT topics. Only 12.3% report cybersecurity as one of the three *least* important subjects—only greater than software engineering. The differential between students who view cybersecurity as one of the three most important subjects and one of the three least important subjects is 4th highest among CIT subjects (+13.4%). However, most participants (60%) do not consider cybersecurity a top three most *or* least important topic. This all indicates students consider cybersecurity a subject of relatively non-controversial (but not top) import within CIT.

Figure 1: Importance of Cybersecurity as Compared to other Computing Subjects



Students also consider cybersecurity to be reasonably important to learn about in CIT, to get a job, and to use throughout their careers, as displayed in table 1. Participants who reported taking cybersecurity courses reported that they had learnt about cybersecurity ($\bar{x}$ = 3.35) while those who had not taken cybersecurity courses reported that they had not ($\bar{x}$ = 1.78), with statistical significance and a high effect size (p-value <.05, Cramer's V >.29), as expected. However, we found no statistically significant relationship between students who took cybersecurity courses and those who hadn't, and in whether students feel that CIT programs should teach about cybersecurity, whether understanding cybersecurity is important to getting a job in CIT, and whether students would expect to use cybersecurity in their careers. This indicates that explicit instruction in cybersecurity is unrelated to student attitudes of its importance, as students consider cybersecurity important regardless of classroom experience.

Table 1: Importance of Cybersecurity in General

Survey Item	N	$\bar{x}$	σ
I have learned about cybersecurity in my coursework so far.	100	2.2	1.08
I would expect computer and information technology programs to teach about cybersecurity.	100	3.2	.70
Understanding cybersecurity is important to securing a job in CIT.	100	2.8	.83
I would expect to use cybersecurity throughout a career in CIT.	100	2.9	.93

4.2 Prior Experience in Cybersecurity is Related to Knowledge of CCs, Excluding Systems Thinking

Students who had previously taken classes in cybersecurity were more likely to report learning about all but one (systems thinking) of the CCs than students who had not, with statistically significant relationships in the chi-squared test ($p<.05$) and high effect sizes (df=3, Cramer's V>.29). This finding suggests that cybersecurity classes are teaching the CCs more so than non-cybersecurity classes, except for systems thinking. Additionally, participants were significantly less likely to understand how system thinking applied to cybersecurity ($p<.05$) as compared to all other CCs, with medium-small to medium effect sizes in t-tests (Cohens-D's from .30 to .57). This indicates that systems thinking may require special attention from other concepts when considering how to increase student understandings of cybersecurity.

4.3 Participants Reported CCs as more Important than Cybersecurity as a Whole

Although few participants reported taking a course covering cybersecurity topics (26%), nearly all recognized the importance of CCs to their future careers and had an expectation that they will or should learn about them. In fact, respondents reported that all the CCs were more important to learn about in CIT, to get a job, and to use in their careers, than cybersecurity in general, regardless of prior cybersecurity experience. As shown in the table 2, many of these differences met the criteria of statistical significance (colored red). All the CCs were reported to be significantly more important than cybersecurity for trying to get a job in CIT ($p<.05$), and in all but one of them (systems thinking) participants were significantly more likely ($p<.05$) to expect to use these concepts throughout a career. These significant results generally paired with medium (Cohen's D~.5) but varied effect sizes (colored orange). Additionally, participants were significantly more likely ($p<.05$) to report having learned about three of the CCs (confidentiality, integrity, availability) than cybersecurity, with the respective effect sizes (D=.32, .56, .43), indicating some participants learned about these concepts without

attributing them to cybersecurity. In our survey CC's were each defined to participants — as many terms are used in other contexts — to ensure construct validity [12].

Table 2: Cybersecurity Concepts

CC	Survey Item	N	x̄	σ	P-Value	Cohen's-D
Confidentiality	I understand how this concept applies to cybersecurity.	91	3.5	.79		
	I have learned about this concept in my coursework so far.	91	2.6	1.13	.006	.324
	I would expect CIT programs to teach about this concept.	91	3.4	.75	.151	.161
	Understanding this concept is important to securing a job in CIT.	91	3.2	.93	.0002	.445
	I would expect to use this concept throughout a career in CIT.	91	3.4	.81	.0004	.427
Integrity	I understand how this concept applies to cybersecurity.	88	3.6	.68		
	I have learned about this concept in my coursework so far.	87	2.9	.97	.00001	.560
	I would expect CIT programs to teach about this concept.	87	3.5	.59	.030	.254
	Understanding this concept is important to securing a job in CIT.	86	3.4	.73	<.00001	.717
	I would expect to use this concept throughout a career in CIT.	87	3.5	.65	<.00001	.596
Availability	I understand how this concept applies to cybersecurity.	87	3.3	.77		
	I have learned about this concept in my coursework so far.	86	2.7	.96	.0003	.429
	I would expect CIT programs to teach about this concept.	87	3.3	.65	.779	.033
	Understanding this concept is important to securing a job in CIT.	86	3.2	.75	.0001	.495
	I would expect to use this concept throughout a career in CIT.	87	3.4	.64	.0003	.461
Risk	I understand how this concept applies to cybersecurity.	85	3.3	.90		
	I have learned about this concept in my coursework so far.	85	2.4	1.05	.35	.108
	I would expect CIT programs to teach about this concept.	85	3.3	.71	.665	.052
	Understanding this concept is important to securing a job in CIT.	85	3.2	.83	.004	.375
	I would expect to use this concept throughout a career in CIT.	83	3.4	.75	.001	.429
Adversarial Thinking	I understand how this concept applies to cybersecurity.	82	3.6	.77		
	I have learned about this concept in my coursework so far.	82	2.3	1.19	.635	.056
	I would expect CIT programs to teach about this concept.	82	3.2	.83	.409	.101
	Understanding this concept is important to securing a job in CIT.	82	3.3	.81	.00002	.585
	I would expect to use this concept throughout a career in CIT.	81	3.4	.75	.013	.322
Systems Thinking	I understand how this concept applies to cybersecurity.	82	3.0	.99		
	I have learned about this concept in my coursework so far.	82	2.4	1.07	.493	.081
	I would expect CIT programs to teach about this concept.	82	3.2	.75	.409	.101
	Understanding this concept is important to securing a job in CIT.	82	3.2	.83	.001	.433
	I would expect to use this concept throughout a career in CIT.	82	3.2	.75	.167	.177

4.4 Participants Confirmed Preconceptions of Cybersecurity from Prior Work

Participants overall confirmed many — but not all — previously observed preconceptions of cybersecurity. As demonstrated in table 3, participants generally agreed that "working in cybersecurity is difficult," "time consuming," "cool," "dominated by men," and "will have a large societal impact". That cybersecurity requires "advanced math skills" and is "accessible to anybody who wishes to learn about it" had more tepid agreement. Participants slightly disagreed that work in cybersecurity requires "a brilliant mind".

Women were more likely than men to assent that work in cybersecurity requires "advanced math skills", with statistical significance and a large effect size ($p < .05$, Cramer's $V > .29$). We also found a result slightly below the threshold of significance with a large effect size ($p = .054$, Cramer's $V > .29$), that men were more likely than women to consider cybersecurity "accessible to anybody who wishes to learn about it". We encourage other researchers to investigate this result in future work.

We also found that participants who reported previous learning in cybersecurity were more likely to consider the topic "cool" ($p=.011$, Cohen's $d = .53$) and "accessible to all" ($p=.034$, Cohen's $d = .51$), with moderate effect sizes. We cannot determine causation; participants may have chosen to take cybersecurity classes because they already held these positive preconceptions, developed these positive preconceptions in their cybersecurity class(es), or some combination of the two.

Table 3: Student Preconceptions of Cybersecurity

Survey Item	N	x̄	σ
Work in cybersecurity is difficult.	116	3.3	.68
Work in cybersecurity is time-consuming.	116	3.3	.67
To do work in cybersecurity, it is important to have advanced math skills.	115	2.8	.88
Cybersecurity is accessible to anyone who wishes to learn about it.	115	3.0	.81
To do work in cybersecurity, it is important to have a brilliant mind.	115	2.2	.83
Cybersecurity is cool.	115	3.2	.76
Cybersecurity is a male-dominated discipline.	115	3.5	.68
Work in cybersecurity will have a large societal impact.	115	3.6	.59

5 DISCUSSION

Multiple stakeholder groups, including governments, tech companies, and educational institutions, have publicly emphasized cybersecurity's importance. Our findings suggest that this messaging may have had its intended impact, as even CIT students without direct experience with cybersecurity recognize the importance of the topic. However, because this perception of importance was unrelated to the choice to take a cybersecurity course (even for students who were done or nearly done with their coursework), we can also speculate that merely emphasizing the importance of the topic may not be sufficient to motivate students to study cybersecurity.

Our findings offer a potential alternative explanation for barriers to student enrollment in cybersecurity; *Many students don't have a clear conception of what exactly cybersecurity is.* This is supported by our results on participant perceptions of the relative importance of CC's when compared with cybersecurity. A lack of clarity about what cybersecurity entails leaves the door open for misconceptions to take hold.

Our results expand prior research on preconceptions of cybersecurity that may dissuade participation, particularly from people from groups underrepresented in computing. Several discouraging preconceptions of cybersecurity ("difficult," "time-consuming," "dominated by men") were reported as prevalent among participants, with one ("requires advanced math skills") more prevalent among women. The discouraging preconception that cybersecurity requires "a brilliant mind" was largely not agreed with by participants. Two more positive preconceptions of cybersecurity ("cool," "will have a large societal impact") were observed, with one more mixed result ("accessible"). We recommend making active efforts to counter negative preconceptions and promote positive ones when speaking about and advocating for cybersecurity to students.

To clarify cybersecurity to potential students as well as leverage the perceived importance of the CCs, classes could be marketed to students with CCs (definitions included) in course descriptions, as well as in other outreach efforts. Additionally, teaching about CCs in non-cybersecurity CIT classes may be an accessible introduction to cybersecurity and pique students' interest in the topic. Similar to adjacent areas of responsible computing such as ethics [16, 33] and accessibility [14], cybersecurity has the potential to be integrated throughout CIT curriculum rather than silo-ed in standalone classes, as suggested by prior work [1, 41]. For topics that are highly relevant to other parts of computing professional practice, such integration has the benefit of ensuring all students have some basic knowledge relevant to their own areas of expertise [13, 33].

For students who may never take a cybersecurity course, there are a number of ways in which these individual components may be incorporated into their other coursework. Prior work has shown how technical assignments in introductory programming courses can be recontextualized to incorporate issues of responsible computing [13]; a simple coding assignment on string matching could be designed to also teach about password strength, introducing concepts of confidentiality. Adversarial thinking can be relevant to any CIT topic where things might go wrong, and can be explored in creative ways [21]. Group projects for topics such as software engineering are often designed to emulate real world scenarios and development work [24] where systems thinking is important for students to practice.

Also, cybersecurity concepts are critical for many areas of emerging technology that may attract students to upper-division coursework. *Inside Higher Ed* reported in mid-2023 that universities are racing to hire and offer coursework in artificial intelligence amid an "AI gold rush" [7]. At the same time, the U.S. government has acknowledged that cybersecurity is an important component of AI education, given how essential it is to leverage cybersecurity practices to guard AI technologies from unintended uses and hostile exploitation [34] and ideas and practices at the intersection of AI and cybersecurity education are beginning to emerge [17, 22].

As revealed by prior work on ethics education in CIT, there may be challenges to this type of integration, including incentive misalignment, lack of training and/or support, and inadequate subject matter knowledge. However, the availability of open resources, community, and departmental support can mitigate many of these challenges [33]. Our results also indicate that one concept, systems thinking— defined as: *"a thinking process that considers how a variety of social and technical constraints intermingle to ensure systems run smoothly*" — may need to be treated differently than the other CCs, given particular attention to ensure students understand it is important individually and as a component of cybersecurity. We recommend that educators consider collaboration and discussion towards a more holistic approach to cybersecurity across their curriculum.

6 FUTURE WORK

Cybersecurity outreach making use of CCs can be investigated through surveys, focus groups, or experimental methods to gain insight to their impact and efficacy in motivating opinions of and enrollment in the topic. The impact of curriculum changes and learning interventions aimed at integrating relevant aspects of cybersecurity in non-cybersecurity CIT classes can also be investigated through these methods. Additionally, future work may aim to understand *why* participants viewed CCs as more important than cybersecurity by gathering rich qualitative data through interviews or focus groups. Further investigation is also needed to understand the impact of negative preconceptions on students' interest in pursuing cybersecurity (e.g., a quantitative study investigating the relationship between endorsing these views and opting to take a cybersecurity course). Finally, conducting a similar study with a larger sample of students underrepresented in CIT and/or in different institutional contexts is an avenue for future work.

ACKNOWLEDGMENTS

Thank you to our survey respondents, the faculty members who forwarded the survey link, and to the National Science Foundation for funding (Award #2115028).

REFERENCES

[1] Blair, J.R.S. et al. 2020. Infusing Principles and Practices for Secure Computing Throughout an Undergraduate Computer Science Curriculum. *Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education* (New York, NY, USA, Jun. 2020), 82–88.

[2] Brauner, P. et al. 2018. Gender influences on school students' mental models of computer science: a quantitative rich picture analysis with sixth graders. *Proceedings of the 4th Conference on Gender & IT* (New York, NY, USA, May 2018), 113–122.

[3] Burley, D. et al. 2017. ACM Joint Task Force on Cybersecurity Education. *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education* (New York, NY, USA, Mar. 2017), 683–684.

[4] By the Numbers | National Center for Women & Information Technology: *https://ncwit.org/resource/bythenumbers/*. Accessed: 2023-07-31.

[5] Cheryan, S. et al. 2017. Why are some STEM fields more gender balanced than others? *Psychological Bulletin*. 143, (2017), 1–35. DOI:https://doi.org/10.1037/bul0000052.

[6] CloudPassage Study Finds U.S. Universities Failing in Cybersecurity Education: 2016. *https://www.globenewswire.com/news-release/2016/04/07/1312702/0/en/CloudPassage-Study-Finds-U-S-Universities-Failing-in-Cybersecurity-Education.html*. Accessed: 2023-08-04.

[7] Colleges Race to Hire and Build Amid AI 'Gold Rush': *https://www.insidehighered.com/news/tech-innovation/artificial-intelligence/2023/05/19/colleges-race-hire-and-build-amid-ai-gold*. Accessed: 2023-07-30.

[8] Computing Classification System: *https://dl.acm.org/ccs*. Accessed: 2023-07-20.

[9] Craigen, D. et al. 2014. Defining Cybersecurity. *Technology Innovation Management Review*. 4, 10 (2014), 13–21.

[10] Cremer, F. et al. 2022. Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance. Issues and Practice*. 47, 3 (2022), 698–736. DOI:https://doi.org/10.1057/s41288-022-00266-6.

[11] Diekman, A.B. et al. 2010. Seeking Congruity Between Goals and Roles: A New Look at Why Women Opt Out of Science, Technology, Engineering, and Mathematics Careers. *Psychological Science*. 21, 8 (Aug. 2010), 1051–1057. DOI:https://doi.org/10.1177/0956797610377342.

[12] Dillman, D.A. 2014. *Internet, Phone, Mail, and Mixed-Mode Surveys*.

[13] Fiesler, C. et al. 2021. Integrating Ethics into Introductory Programming Classes. *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education* (New York, NY, USA, Mar. 2021), 1027–1033.

[14] Gellenbeck, E. 2005. Integrating accessibility into the computer science curriculum. *Journal of Computing Sciences in Colleges*. 21, 1 (Oct. 2005), 267–273.

[15] Goutam, R.K. Importance of Cyber Security. *International Journal of Computer Applications*. 111, 7.

[16] Grosz, B.J. et al. 2018. Embedded EthiCS: Integrating Ethics Broadly Across Computer Science Education. arXiv.

[17] Grover, S. et al. 2023. Cybersecurity Education in the Age of AI: Integrating AI Learning into Cybersecurity High School Curricula. *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1* (New York, NY, USA, Mar. 2023), 980–986.

[18] Hajny, J. et al. 2021. Framework, Tools and Good Practices for Cybersecurity Curricula. *IEEE Access*. 9, (2021), 94723–94747. DOI:https://doi.org/10.1109/ACCESS.2021.3093952.

[19] Jang-Jaccard, J. and Nepal, S. 2014. A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*. 80, 5 (Aug. 2014), 973–993. DOI:https://doi.org/10.1016/j.jcss.2014.02.005.

[20] Joint Task Force On Cybersecurity E 2018. *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. ACM.

[21] Klassen, S. and Fiesler, C. 2022. "Run Wild a Little With Your Imagination": Ethical Speculation in Computing Education with Black Mirror. *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education - Volume 1* (New York, NY, USA, Feb. 2022), 836–842.

[22] Laato, S. et al. 2020. AI in Cybersecurity Education- A Systematic Literature Review of Studies on Cybersecurity MOOCs. *2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT)* (Jul. 2020), 6–10.

[23] Lewis, C.M. et al. 2011. Deciding to major in computer science: a grounded theory of students' self-assessment of ability. *Proceedings of the seventh international workshop on Computing education research* (New York, NY, USA, Aug. 2011), 3–10.

[24] Li, Y. et al. 2022. Student Engagement in Software Engineering Group Projects: An Action Research Study. *Proceedings of the 2022 5th International Conference on Education Technology Management* (Lincoln United Kingdom, Dec. 2022), 367–374.

[25] Li, Y. and Liu, Q. 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*. 7, (Nov. 2021), 8176–8186. DOI:https://doi.org/10.1016/j.egyr.2021.08.126.

[26] LibGuides: Statistics Resources: Cohen's d: *https://resources.nu.edu/statsresources/cohensd*. Accessed: 2023-08-15.

[27] Liu, X. et al. 2022. Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology*. 13, (Oct. 2022), 927398. DOI:https://doi.org/10.3389/fpsyg.2022.927398.

[28] McHugh, M.L. 2013. The Chi-square test of independence. *Biochemia Medica*. 23, 2 (Jun. 2013), 143–149. DOI:https://doi.org/10.11613/BM.2013.018.

[29] Nadler, J.T. et al. 2015. Stuck in the Middle: The Use and Interpretation of Mid-Points in Items on Questionnaires. *The Journal of General Psychology*. 142, 2 (Apr. 2015), 71–89. DOI:https://doi.org/10.1080/00221309.2014.994590.

[30] Ojha, V. et al. 2023. Computing Specializations: Perceptions of AI and Cybersecurity Among CS Students. *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1* (New York, NY, USA, Mar. 2023), 966–972.

[31] Parrish, A. et al. 2018. Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* (Larnaca Cyprus, Jul. 2018), 36–54.

[32] Secure and Trustworthy Cyberspace (SaTC): 2021. *https://new.nsf.gov/funding/opportunities/secure-trustworthy-cyberspace-satc*. Accessed: 2023-07-21.

[33] Smith, J.J. et al. 2023. Incorporating Ethics in Computing Courses: Barriers, Support, and Perspectives from Educators. *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1* (New York, NY, USA, Mar. 2023), 367–373.

[34] Sridhar, N. et al. 2021. Cybersecurity Education in the Age of Artificial Intelligence. *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education* (New York, NY, USA, Mar. 2021), 1365.

[35] Švábenský, V. et al. 2020. What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences. *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (Feb. 2020), 2–8.

[36] There Are Too Few Women in Computer Science and Engineering: *https://www.scientificamerican.com/article/there-are-too-few-women-in-computer-science-and-engineering/*. Accessed: 2023-07-30.

[37] Threat Landscape: *https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends*. Accessed: 2023-07-21.

[38] Tsvetanov, T. and Slaria, S. 2021. The effect of the Colonial Pipeline shutdown on gasoline prices. *Economics Letters*. 209, (Dec. 2021), 110122. DOI:https://doi.org/10.1016/j.econlet.2021.110122.

[39] Unfried, A. et al. Gender and Student Attitudes toward Science, Technology, Engineering, and Mathematics.

[40] Verdugo-Castro, S. et al. 2022. University students' views regarding gender in STEM studies: Design and validation of an instrument. *Education and Information Technologies*. 27, 9 (Nov. 2022), 12301–12336. DOI:https://doi.org/10.1007/s10639-022-11110-8.

[41] White, G.B. et al. 1999. Incorporating security issues throughout the computer science curriculum. *Proceedings of the IFIP TC11 WG 11.8 First World Conference on Information Security Education* (1999), 19–26.

[42] Wolff, J. 2016. Why Computer Science Programs Don't Require Cybersecurity Classes. *Slate*.

[43] Women in Computer Science & Programming | ComputerScience.org: 2022. *https://www.computerscience.org/resources/women-in-computer-science/*. Accessed: 2023-07-30.

[44] Zach 2020. Fisher's Exact Test: Definition, Formula, and Example. *Statology*.

[45] Zach 2021. How to Interpret Cramer's V (With Examples). *Statology*.

[46] 2018. Criteria for Accrediting Computing Programs. ABET Computing Accreditation Commission.

[47] Vision Statement – CS2023.