

A Case Study-based Cybersecurity Ethics Curriculum

Jane Blanken-Webb, Imani Palmer, Sarah-Elizabeth Deshaies
Nicholas C. Burbules, Roy H. Campbell, Masooda Bashir
University of Illinois at Urbana-Champaign

Abstract

This paper describes the rationale for and implementation of an experimental graduate-level cybersecurity ethics course curriculum recently piloted at the University of Illinois at Urbana-Champaign. This case study-based ethics curriculum immerses students in real-life ethical dilemmas within cybersecurity and engages in open dialogue and debate within a community of ethical practice. We uphold the importance of preparing students for a future that is truly unknown and uncertain and note that this requires a push beyond some established curricular guidelines for cybersecurity that underlie a rule and compliance-based approach to ethics education. Details of the course layout are offered as well as results from a student-evaluation survey.

1 Introduction

Given the gravity, complexity, and vast array of ethical dilemmas within cybersecurity, we maintain that cybersecurity ethics now merits its own curricular focus in preparing cybersecurity professionals. To address this need, we recently developed and piloted a graduate-level cybersecurity ethics curriculum at the University of Illinois at Urbana-Champaign.

We uphold the value of thinking through complex ethically-laden scenarios in cybersecurity and developed a case-study based ethics curriculum to engage students in open dialogue and debate within a community of ethical practice. Being proactive is important in order to make any system more secure and in the realm of cybersecurity ethics, we are concerned with the system of people (i.e. cybersecurity professionals) who are situated on the front line of ethical and technological decisions that stand to shape the future of society. We recognize that the midst of a cybersecurity crisis is arguably a suboptimal time to initiate rich, thorough, and detailed dialogue related to the ethical implications of a given sit-

uation. Therefore, this course aspires to expose students to the nuances of complex cases in cybersecurity ahead of time—before they are the ones situated on the technological edge.

However, creating an ethics curriculum that can prepare students for a future that is truly unknown and uncertain requires that we push beyond established curricular guidelines for cybersecurity ethics that underline a rule and compliance-based approach. In short, we maintain that memorizing relevant laws and codes of ethics is not ethics education. Or, at the very least, it is not the kind of ethics education that will prepare the urgently needed decision makers of tomorrow in the realm of cybersecurity.

The rest of the discussion is organized as follows. Section 2 discusses background information related to cybersecurity education and the need for a specific curricular focus on cybersecurity ethics. Section 3 provides an overview of the major curricular guidelines that have been proposed for cybersecurity as they relate to the experimental curriculum discussed in this paper. Section 4 describes in more detail the curricular approach undertaken in relation to established ethical frameworks. Section 5 offers a discussion of challenges and implications related to this initiative and Section 6 is a conclusion and discussion of future work.

2 Background

As society becomes ever-more reliant on cyber infrastructures to manage crucial aspects of daily living, threats posed by cyber-attacks become increasingly critical. In response to this, federal funding on national security has increased for cybersecurity initiatives. For example, the 2017 Federal Budget allocated \$19 billion for cybersecurity, an over 35% increase from 2016 [8, 16, 20, 33]. However, the annual number of successful cyber attacks continues to increase [20, 22, 33]. Given this re-

ality, we seem no closer to ensuring reliable safety in our private, corporate, and governmental digital information systems.

Despite increased national attention and funding for cybersecurity, one of the primary factors in the development of cybersecurity protections is the lack of skilled cybersecurity professionals. Current estimates indicate a global shortfall of skilled cybersecurity professionals that will number 1.5 million by 2019 [13].

There are substantial efforts underway to address the demand to develop this workforce [10, 24]. However, in the rush to meet the need to prepare these future cybersecurity professionals, it is vital that we maintain a holistic view of the education these professionals require [15].

This cybersecurity workforce will be on the forefront of ethical conundrums that stands to shape the future of society. Yet, many information technology and cybersecurity professionals do not realize how their jobs entail significant ethical dilemmas despite the reality that they are placed in positions to make decisions on a daily basis that raise substantial ethical questions [14, 28, 31]. Cybersecurity professional need to recognize and understand that technology is far from being value-free: “Any technological decision... is a value-based decision that not only reflects a particular vision of society but also gives concrete form to it” [9]. We are educating custodians of information who have access to things like private emails, geolocation, web purchasing patterns, social networking information, and web browsing histories. These professionals are situated on the frontline of ethical decisions about whether and under what conditions to access and use this information. Is it ethical to keep a record of this kind of personal data with or without users awareness? On the other hand, is it ethical to ignore or delete this information when it has the potential to provide alerts to subversive or dangerous activities? Moreover, if we are to collect this information — information that has been deemed a “toxic asset” [30] what kind of responsibility is entailed for protecting it? Placed in the thick of these and many other binds, cybersecurity professionals face a heavy ethical burden that comes along with their increased access and skill.

Amplifying this burden even further is the inability of our society and legal system to cope with the speed of technological innovation. While quick to pick up all the latest computing devices, society as a whole remains mostly oblivious to the data by-product that results from using them [29]. Meanwhile, our legal system moves at a slow pace. The few laws we do have in this area, chief among them being the 1986 Computer Fraud and Abuse Act (CFAA), struggle to “regulate a space where, fundamentally, some of the activities we want to encourage among the good guys finding new vulnerabilities in computer systems, testing the security of software

and devices are largely indistinguishable from the activities that we want to discourage when undertaken by the bad guys” [34]. Investigations into cyber attacks rarely lead to prosecutions and therefore have little deterrence value: “In comparison to other federal crimes, CFAA offenses are not charged frequently and prosecuting someone engaged [in] computer security research is extremely rare” [5].

Cybersecurity professionals are situated in a position to make crucial decisions in the midst of professional practice, often with little guidance. Unlike more established professions like medicine or law, cybersecurity does not have codified standards of ethics — nor is cybersecurity anywhere near establishing such standards. Researchers in cybersecurity lack agreement upon common ethical principles and some remain unconvinced of the value, or even the possibility, of establishing a universal framework that can address the realm of cybersecurity [19]. Given this complex situation, it is imperative that cybersecurity professionals are educated in a way that cultivates and develops wide-ranging capacities, skills, and dispositions that will prepare them to recognize and cope with the ethical and technological conundrums before them.

3 Related Work

The importance of incorporating ethics education within the preparation of cybersecurity professionals is reflected in three significant curricular frameworks and guidelines that have recently been proposed for cybersecurity education: The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [26], the Centers of Academic Excellence (CAE) in Cyber Security Core Knowledge Units (2018), and Cybersecurity Curricula 2017 [7], put forth by the Joint Task Force on Cybersecurity Education. This section will consider these curricular frameworks as well as the Certified Ethical Hacker curriculum in relation to our experiential curriculum.

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework includes knowledge of ethical hacking principles and techniques as well as knowledge of national and international laws, regulation, policies and ethics as they relate to cybersecurity [26]. While knowledge of laws and policies are an important place to begin, we maintain that the NICE Framework does not go far enough in emphasizing the crucial role of ethics education in the preparation of cybersecurity professionals. In addition to imparting knowledge of relevant laws and ethical principles and practices, there is a need to cultivate wide-ranging capacities, skills, and dispositions that will enable cybersecurity professionals to utilize, reflect upon, and revise

this knowledge-base throughout their careers.

Similarly, the recently established CAE Knowledge Units include a Core Knowledge Unit called Policy, Legal, Ethics, and Compliance. This knowledge unit intends “to provide students with an understanding of information assurance in the context of the rules and guidelines that controls them,” [1] by having students list and describe applicable laws and policies, which includes responsibilities for handling vulnerabilities. However, as laid out in Section 2, we maintain that the context of information assurance (or cybersecurity) is not well contained by rules and guidelines. Ethics education in this realm needs to do more than impart rules and insist upon compliance.

Other established curriculums such as Certified Ethical Hacker (EC-Council) [12] also focus on a rule and compliance-based approach to ethics, offering a training in hacking techniques within a framework of rules that are deemed to be “ethical.” Ethical conduct in this type of certification training refers to clearly defined procedures that align with specific methodologies and policies that essentially amount to following rules correctly. While it is important for cybersecurity students and professionals to be aware of these rules and to follow them when they are applicable to specific situations, we maintain that such training is not innovative enough for the education cybersecurity professionals need. It is not sufficient to simply teach clearly defined rules in the realm of cybersecurity because the speed of technological innovation is moving much faster than rules can keep up with. In an arena where the rules that are changing all the time, we need to think about ethics education in new and innovative ways that recognize how,

many of the most daunting and important ethical issues individuals and societies face are those arising from new technologies that can create situations that humans haven't faced before. These are precisely the kinds of ethical questions that cannot be decided by social convention because there are no absolute rules and practices that precisely apply [18]

The Joint Task Force on Cybersecurity Education (JTF) represents another initiative to develop comprehensive curricular guidance in cybersecurity education with their Cybersecurity Curricula 2017 [7]. This initiative incorporates ethics within their very definition of cybersecurity and builds upon a conception of ethics that goes well beyond rule following and compliance. Cyberethics is included among their Societal Security Knowledge Area, which features a rich array of topics that explicitly acknowledges distinctions between the realm of law and the realm of ethics. Cybersecurity Curricula 2017 [7], lays firm groundwork supporting the ap-

proach taken in our experimental case study-based cybersecurity ethics curriculum.

4 Experimental Curriculum

Our case study-based ethics curriculum for cybersecurity immerses students in real-life ethical dilemmas inherent to cybersecurity. Students engage in open dialogue and debate engaging complex dimensions of cybersecurity case studies. The curriculum is designed to develop critical ethical reasoning skills in addition to skills vital for cybersecurity professionals.

The specific curricular objectives and the expected areas of impact include:

- Increased awareness of the complex web of consequences that cybersecurity professionals are prone to encounter
- Increased awareness and reflection upon students personal ethical inclinations
- Development of critical reasoning skills that will allow students to become more sophisticated in their ethical reasoning abilities and responses
- Development of collaborative problem solving and communication skills
- Fostering and establishing a culture of dialogue around complex ethical dimensions of cybersecurity

The pilot graduate-level course was taught in Spring 2018. The class consisted of one 3-hour class session each week for a 16- week term. The course topics for this course are listed in Table 1. These course topics were reviewed and suggested by a committee of people from various disciplines in computer science, computer engineering, information science, philosophy, and education.

The grading scale includes participation, homework assignments, midterm project proposal, and a final group project. The participation grade includes class preparation, attendance, and participation. The course has six homework assignments shown below in Table 3.

4.1 Case Study-based Approach

Our curriculum is designed to assist students in clarifying and applying their ethical values as they encounter new, complex situations where it may not be obvious how ethical values may apply or where the appropriate application of one of these values may conflict with other ethical values [27]. To prepare them for such contexts, we need richly described, realistic accounts of complex ethical dilemmas that arise within the practice in which protagonists must decide among courses of action, none of

which is self-evident as the right one to take [23]. Meira Levinson and Jacob Fay offer that working through complex cases foster the development of the kind of practical reasoning (phronesis) that constitutes a marriage of theory and practice. They argue, in fact, that practical ethical judgment can best be fostered through this case-based method.

The value of engaging complex case-studies that are not straightforwardly solvable lies in a cumulative ongoing process of improving understandings and capacities (sometimes through error and correction). We strive to stimulate honest conversations amongst the very actors who will be on the forefront of these crucial ethical conundrums in their professional futures. In this, students in this course practiced the skills and dispositions we want to cultivate for the entire cybersecurity community. An intentional and integral aspect of our approach is to engage in group dialogue. This is because group discussion supports deeper and multifaceted critical thinking, which offers both pedagogical and analytical benefits. And by engaging these complex ethical issues within a critically-engaged community, we are ultimately striving to foster and establish a broader culture of dialogue among cybersecurity professionals to collectively determine the best paths forward. The case studies used in the course are shown below in Table 4.

It is important to recognize that there are no once-and-for-all, absolute solutions in the realm of cybersecurity. As expressed by William H. Sanders [2], cybersecurity is an area in which we should aim for a pragmatic, but not the perfect approach. Accordingly, we need to replace the quest for absolute certainty by cognitive means with the search for security by practical means [11]. This is not just a matter of recognizing that we can never fully attain our ideals; rather, we need ways of thinking about how to choose and act in a context that is intrinsically limited. The proposed case study approach offers just that, a way of considering the specifics of limited situations and contemplating the nuances of particular cases.

Rather than assuming the vocabulary of applying philosophical tools to cybersecurity problems, we invert the order of things, beginning with concrete and richly detailed case studies and examples, and drawing philosophical insights from the analysis of those particulars. While principles certainly play a role, in the realm of cybersecurity practitioners are at the forefront of making judgments about where, how much, and in what respects the present case is similar to precedents. Accordingly, our curriculum is designed to assist students in clarifying and applying their ethical values as they encounter new, complex situations where it may not be obvious how ethical values may apply or where the appropriate application of one of these values may conflict with other ethical values [27].

4.2 Ethical Thinking

Ethics encompasses a broad realm of human inquiry engaging fundamental questions that ultimately seek to answer what it means to live a good life. Within the Western philosophical tradition, there are three main ethical frameworks: deontological ethics, consequentialist ethics, and virtue ethics. These three approaches offer valuable and competing perspectives for thinking about how to determine ethical value. Although these frameworks provide a good place to start for thinking about ethics, the cutting-edge nature of cybersecurity pushes upon the limits of all of these frameworks. Moreover, it is vital to consider a global perspective for engaging in ethical thinking in cybersecurity. We maintain the value of incorporating as many perspectives as possible into well-grounded ethical inquiry sustained through dialogue. In the end, our approach to ethics is open-ended in that we are not proposing a single solution or method of reasoning. Rather, we uphold the significance of creating intentional space for engaging in a cumulative and ongoing process of ethical inquiry that can hold the field of cybersecurity such that a needed degree of cohesiveness is maintained in order to allow it to move forward as it confronts new ground.

The ethical frameworks addressed in the class are listed in Table 2. Notably, we also consider meta-ethical frameworks of ethical absolutism, ethical relativism, and ethical pluralism. While we do not dictate the precise framework people must use in analyzing case studies, we are advocating for an overall meta-framework of ethical pluralism in this course.

Below we briefly introduce the three most established ethical frameworks within the Western philosophical tradition: Deontological Ethics, Consequentialist Ethics, and Virtue Ethics. Deontological ethics engage moral theories that guide and assess our choices in relation to duty, what we ought to do. Deontological ethics are concerned with the moral value of actions taken, rather than with their consequences or with the kind of person we are or should be [3]. In a general sense, ethical codes provide an example of deontological ethics as moral value is placed in following rules.

Consequentialist ethics are concerned with the outcomes or consequences of an act. Utilitarianism offers the paradigmatic case of consequentialism in which actions that bring about good consequences are of moral value. Consequentialist theories define what is good in various ways, but it is common to say that the good refers to consequences that bring about the greatest happiness for the greatest number [32].

Virtue ethics stems from the fundamental concern of being a good person. Virtue ethics address a person's disposition and refers to long enduring character traits.

Practical wisdom (or phronesis) is an important subcategory of virtue ethics and concerns practical virtues such as having the necessary knowledge or understanding that allows an individual to act well specific situations [17, 4]. According to Aristotles formulation, phronesis is both necessary and sufficient for being a virtuous person. It is not enough to learn general principles of action. We need to acquire and practice deliberative, emotional, and social skills that will allow us to put general principles into practice in ways that are well-suited to particular situations [21, 6].

Moral philosophy cannot be simply an examination of what it is right or wrong to do, without asking whether and how it is possible to actually foster the development of people who will think and act that way. Hence, it is important for cybersecurity educators to not only cultivate capacities and skills for ethical reasoning, but also to cultivate dispositions to utilize these skills well. Dialogue and ethical consideration within community is therefore key in ethics education. This can foster a social ethos of care that will be grounded in lived relationships of cooperation and mutual accountability within community. Establishing a culture of dialogue in which complex ethical issues can be worked through in ideation prior to action stands to increase assurance that ethical decisions will be well thought through and informed by diverse perspectives. Cybersecurity needs to foster a culture in which cybersecurity professionals hold each other accountable, but who also learn from ethical missteps and grow as a community as a result of lessons learned. This is our aim in this experimental case-study based cybersecurity ethics curriculum.

4.3 Evaluation Methodology

At the conclusion of the course, and with IRB approval, students were surveyed to evaluate the effectiveness of the course in realizing its aims. The evaluation survey focused on five areas: the course in general, the homework assignments, the final group project, the course topics, and the students experience with this course. The goal of the evaluation is to gather information about the students perspectives, experiences, and suggestions. The survey included free response questions, likert scale ratings, and multiple choice selections. In total, 14 students of mixed genders responded to most of the survey.

5 Evaluation

The results shown below are based on a post-course evaluation survey of the teaching of the initial experimental course. Below, we provide a summary of the

findings and opportunities to reflect upon and improve the curriculum.

5.1 General Course Feedback

In an open-ended question, students were asked to provide feedback on the importance of the course; about four students commented on how this course helps students become aware of ethical issues in cyberspace. One student commented, “this course is important because it initiates dialogues and discussions of ethical case studies and situations that are inevitable in real life. By covering these topics, people can have prior experience and thus more likely to be making decisions that are thought through when they face a similar experience”. Other students commented on the importance of viewing cybersecurity from a non-technological view, “[this course] fills a gap that is not covered in existing courses by addressing the human factors in security”.

Students spent an average of five hours a week outside of class time (range: 2-10 hours). Five students responded that they wish they had spent more time on this course, many citing that they desired more depth on some issues. On a likert scale, students rated an average 4.78/5 that they were able to complete the weekly homework assignments on time. Furthermore, the homeworks were rated a 4/5 as effective for engaging with the topics inside of class, but a 3.71/5 as somewhat effective in their ability to engage with the topics outside of class. The major strengths of the homeworks were their relevance to the field and to todays cyber security issues. Some of the weaknesses of the assignments had to do with either their redundancy, or with specific topics being difficult to engage with through assignments such as cyberwarfare. However, nine out of thirteen students reported that the homework overall helped their learning.

Students were asked “did the evaluation of case studies help your understanding of ethical frameworks?”, thirteen of fourteen students responded “yes”. When asked which case studies were most helpful, many students responded similarly with the top four being “The Ones That Walked Away From Omelas”, “Apple Vs FBI”, “The Morris Worm”, and “The Racist Soap Dispenser.”

As for the final group project, students found this to be an effective learning strategy with a rating of 4.28 out of five, (five being very effective). One student elaborated stating, “I was able to talk with other people and understand their perspective. This was a great learning experience that I wouldnt have had anywhere else”. Most students (12 out of 12 responding) also agreed that future classes should have a group project, one student commented, “this class is intended for fostering communication, this cant be done in a vacuum”.

When given the opportunity for feedback in various

places, students noted that they struggled with the last minute changes to readings, the lack of group project ideas, the lack of discussion moderation, and the length of the class. Many of these dislikes originated from the novelty of the course and its first offering and will be resolved in future offerings. As for our learning objectives (results are shown in Table 5), we found that students found that facilitating a culture of dialogue was the most successful learning objective met by this course (average rating 4.93/5). The second most successful was the courses ability to increase their awareness of ethical dilemmas in cybersecurity (average 4.36/5). This course was found to be least successful in increasing collaborative problem solving skills (3.07/5) and increasing professional judgement of ethical issues (3.64/5).

5.2 Future Courses

We also asked the students “what impacts do you think this course stands to have for future students?” and one student commented that this course “may help to awaken passions within the field”. Other students commented on how being aware of these ethical dilemmas may help them make better decisions in the future. Students were then asked about the impact this course may have for future companies, to which one student replied, “technological tools and advances can benefit greatly from being judged from an ethical lens before development (so Cabridge Analytica doesnt happen).”

When asked about future courses like this one, six students out of thirteen felt as though this course could be taught at both a graduate level and an undergraduate level. Furthermore, ten out of twelve felt as though this course should be required for students who plan to work in the field of cybersecurity. All students who responded to the survey agreed that there should not be a required textbook for this type of course. A few students suggested that required readings should be kept up-to-date with new developments and broken up into sizeable chunks. Another student suggested “the readings should be tiered: required, optional, and supplementary. By giving urgency and importance, students will be able to prioritize the readings.” Finally, twelve out of twelve students responding agreed that the final project should be done as a group, and that there should be check-in points throughout the semester to hold all students in the group accountable.

As for the time spent in class, students commented that a three hour block of class was a bit long. One student also commented “[a] class style of approx 15-20 minutes [per discussion topic] is perfect to facilitate discussion and involve everyone.” Another student commented “I liked the broad review aspect. It would be interesting to cover an emerging issue each week for 10-15 minutes to

show practical application.”

We asked students to evaluate each course topic individually, rating them on their difficulty, when each topic should be covered, and how essential each topic was (see Figures 1, 2, 3). As we can see “Professional Responsibility in Cybersecurity Research and Industry” was rated at the most difficult topic. This topic was also rated as one of the most important topics alongside “Intro to Cybersecurity/Socio-Technical Computer Ethics”, “Intro to Ethical Frameworks”, and “Privacy”. When students were asked which topics they wished had been covered in more depth, most students responded with “Privacy”, “Codes of Ethics”, and “Security”.

Finally, as for suggested topics, students responded with an interest in “security marginalized groups (e.g. LGBTQ+)”, “International Cybersecurity”, and “ethics of censorship bypass”.

5.3 Discussion

The development of this curriculum did not come without challenges. One main challenge with this overall initiative is to introduce ethical reflection into a field that is widely seen as purely technical. We are resisting the notion that professional and job-specific demands may override important ethical considerations that distract from the task at hand. “The challenge computer educators face is to develop strategies that will raise the awareness of students regarding ethical and moral issues related to computer technology at the same time that they are developing their technical expertise” [25]. We need to develop the attitude that these considerations are intrinsic, not extrinsic: working from real-life case studies is a key part of this instructional strategy. Diving into complex case studies allows students to grasp the technical possibilities while exploring the ethical challenges simultaneously.

Another challenge is the necessarily multidisciplinary approach this initiative requires in working to find effective ways of addressing the complex realm of cybersecurity ethics. This project incorporates technical, philosophical, educational, and organizational strands in order to be effective. In order to tackle this challenge, we created a multidisciplinary team that comprises these areas of expertise.

This course is broadly developmental in that its primary aim is to develop students as ethical agents. Given this, the course drew upon a pedagogical approach that emphasizes an intuitive and receptive mode of thinking and being in order to support enduring ethical growth and development. While specific predefined knowledge and skills have a role in this course, it should be understood that these items hold a significance that is secondary to the primary and overarching aim. More than simply be-

ing a guide to ethical behavior, this course aimed to establish a method of decision making that can support students for years to come by developing a way of thinking about ethics in complex and undefined spaces.

6 Conclusion & Future Work

In this paper, we described the rationale for and implementation of an experimental graduate-level cybersecurity ethics curriculum recently piloted at the at the University of Illinois at Urbana-Champaign. This case study-based curriculum positions students to grapple with the gravity, complexity, and vast array of ethical dilemmas in cybersecurity that are becoming ever-more pervasive in the digital era. We maintain that cybersecurity ethics now merits its own curricular focus in preparing cybersecurity professionals and propose our experiences with this experimental course in cybersecurity ethics in order to enliven discussion and inform the community of our work with this important initiative.

Future work will include analysis of data from cybersecurity educators for further development and improvements on the course. Moving forward, we plan to expand this curricular initiative to a variety of contexts in order to educate K-12, community college, undergraduate as well as professionals all of which constitute areas where cybersecurity and cyberspace issues get introduced and/or implemented. We recognize that these are quite different educational (and developmental) contexts and invite collaboration with those representing these different sectors.

In cybersecurity education, we are educating the decision makers of the future and we need to create novel pedagogical approaches that will holistically prepare students for their future roles as cybersecurity professionals.

7 Acknowledgments

Project sponsored by the National Security Agency under Grant Number H98230-17-1-0347. The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation herein.

References

- [1] Policy, legal, ethics and compliance. <https://www.caecommunity.org/resources/ku-cards/ku/policy-legal-ethics-and-compliance>. Accessed: 2014-12-09.
- [2] Engineering in cyber resiliency: A pragmatic but not perfect approach. Presentation, 2016.
- [3] ALEXANDER, L., AND MOORE, M. Deontological ethics.
- [4] ATHANASSOULIS. Virtue ethics, 2017.
- [5] BAILEY, M., DITTRICH, D., KENNEALLY, E., AND MAUGHAN, D. The menlo report. *IEEE Security & Privacy* 10, 2 (2012), 71–75.
- [6] BARNES, J. Introduction to aristotle the nicomachean ethics ('ethics'). *Harmondsworth: Penguin* (1976).
- [7] BURLEY, D. L., BISHOP, M., BUCK, S., EKSTROM, J. J., FUTCHER, L., GIBSON, D., HAWTHORNE, E., KAZA, S., LEVY, Y., MATTORD, H., ET AL. Cybersecurity curricula 2017. *Version 0.75 Report 12* (2017).
- [8] CALMES, J. Obamas last budget, and last budget battle with congress. *The New York Times* (2016).
- [9] CHRISTENSEN, K. Ethics of information technology. *The human edge: Information technology and helping people* (1986), 72–91.
- [10] DAWSON, M., WANG, P., AND WILLIAMS, K. The role of cae-cde in cybersecurity education for workforce development. In *Information Technology-New Generations*. Springer, 2018, pp. 127–132.
- [11] DEWEY, J. The quest for certainty: A study of the relation of knowledge and action. *The Journal of Philosophy* 27, 1 (1930), 14–25.
- [12] EC-COUNCIL. Certified ethical hacker. <https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>.
- [13] FURNELL, S., FISCHER, P., AND FINCH, A. Can't get the staff? the growing need for cyber-security skills. *Computer Fraud & Security* 2017, 2 (2017), 5–10.
- [14] GUPTA, U. What is the role of ethics? organizations put new emphasis on staff's ethical behavior. <https://www.bankinfosecurity.com/what-role-ethics-a-3821>. Accessed: 2011-07-06.
- [15] HOFFMAN, L., BURLEY, D., AND TOREGAS, C. Holistically building the cybersecurity workforce. *IEEE Security & Privacy* 10, 2 (2012), 33–39.
- [16] HOUSE, W. Fact sheet: Cybersecurity national action plan. *The White House. February 9* (2016).
- [17] HURHOUSE, R., AND PETTIGROVE, G. Virtue ethics, 2016.
- [18] JOHNSON, D. G., AND MILLER, K. W. *Computer Ethics: Analyzing Information Technology*. Pearson Education International, 2009.
- [19] KENNEALLY, E., AND BAILEY, M. Cyber-security research ethics dialogue & strategy workshop.
- [20] KNOTT, B. A., MANCUSO, V. F., BENNETT, K., FINOMORE, V., MCNEESE, M., MCKNEELY, J. A., AND BEECHER, M. Human factors in cyber warfare: Alternative perspectives. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (2013), vol. 57, SAGE Publications Sage CA: Los Angeles, CA, pp. 399–403.
- [21] KRAUT, R. Aristotle's ethics.
- [22] KURANDA, S. The 10 biggest data breaches of 2015 (so far). *CRN. Retrieved from http://www.crn.com/slideshows/security/300077563/the-10-biggest-data-breaches-of-2015-so-far.htm/pgno/0/10 Google Scholar* (2015).
- [23] LEVINSON, M., AND FAY, J. *Dilemmas of Educational Ethics: Cases and Commentaries*. ERIC, 2016.
- [24] LIEBROCK, L. M. Education: Scholarship for service. *IEEE Distributed Systems Online* 7, 9 (2006), 2–2.
- [25] MARTIN, C. D., AND MARTIN, D. H. Professional codes of conduct and computer ethics education. *Social Science Computer Review* 8, 1 (1990), 96–108.

- [26] NEWHOUSE, B., KEITH, S., SCRIBNER, B., AND WITTE, G. Nice cybersecurity workforce framework (ncwf). *National Institute of Standards and Technology (NIST), Ed., ed. Gaithersburg, MD* (2016).
- [27] PARKER, D. B., SWOPE, S., AND BAKER, B. N. Ethical conflicts in information and computer science, technology, and business.
- [28] RELKIN, J. 10 ethical issues confronting it managers. <https://www.techrepublic.com/article/10-ethical-issues-confronting-it-managers/>. Accessed:2006-08-15.
- [29] SCHNEIER, B. *Data and Goliath: The hidden battles to collect your data and control your world*. WW Norton & Company, 2015.
- [30] SCHNEIER, B. Data is a toxic asset, 2015.
- [31] SHINDER, D. Ethical issues for it security professionals. <https://www.computerworld.com/article/2557944/security0/ethical-issues-for-it-security-professionals.html>. Accessed: 2005-08-02.
- [32] SINNOTT-ARMSTRONG, W. Consequentialism.
- [33] VIEANE, A., FUNKE, G., GUTZWILLER, R., MANCUSO, V., SAWYER, B., AND WICKENS, C. Addressing human factors gaps in cyber defense. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (2016), vol. 60, SAGE Publications Sage CA: Los Angeles, CA, pp. 770–773.
- [34] WOLFF, J. The hacking law that can't hack it. http://www.slate.com/articles/technology/future_tense/2016/09/the_computer_fraud_and_abuse_act_turns_30_years_old.html. Accessed: 2016-09-27.

A Appendix

Course Topics
Introduction to Cybersecurity
Socio-technical Computer Ethics
Introduction to Ethical Thinking
Ethical Issues in Cybersecurity Education
Cybersecurity and Society
Codes of Ethics
Professional Responsibility in Cybersecurity
Incident Response
Hacking Back
Responsible Disclosure
Whistleblower, Leaker
Insider Threat
Law & Ethics
Privacy
Information, Propaganda, Misinformation & Disinformation
Cyberwarfare
The Future of Cyber

Table 1: The list of course topics

Ethical Frameworks	Meta-Ethical Frameworks
Deontological Ethics	Ethical Relativism
Consequentialist Ethics	Ethical Monism/Absolutism
Virtue Ethics	Ethical Pluralism
Rights & Social Contract	
Feminist Ethics of Care	
Pragmatist Ethics	
Confucian Ethics	

Table 2: Ethical frameworks discussed in the course

Homework Assignments	Descriptions
Ethical Framework Identification	Identify which ethical frameworks reflect your own decision making Identify which ethical frameworks do not Discuss the meta-ethical frameworks that you would apply
Ethical Decision in Cybersecurity Education	Select a skill taught in cybersecurity education Discuss how to teach this skill Respond to other students discussions
Cybersecurity and Society Case Study	Develop a case study scenario that centers on an ethical dilemma Respond to other students discussions
Code of Ethics	Review and critique a code of ethics related to cybersecurity Discuss any gaps and codes that violate your ethical framework
Codes of Ethics One Step Further	Construct a new code of ethics for a particular cybersecurity domain Respond to the code of ethics of other students
Responsible Disclosure Mind Map	Construct a new code of ethics for a particular cybersecurity domain Respond to the code of ethics of other students
Reflective Ethical Framework Identification Essay	

Table 3: The homework assignments and descriptions of the course

Course Topics	Case Studies	Description
Introduction to Cybersecurity Socio-Technical Computer Ethics	Slaughterbots	A dramatized near-future scenario where swarms of inexpensive microdrones use artificial intelligence and facial recognition to assassinate political opponents based on pre-programmed criteria
Introduction to Ethical Thinking & Ethical Decision Making	The Ones Who Walk Away From Omelas	A description of a summer festival in the utopian city of Omelas whose prosperity depends on the perpetual misery of a single child
Ethical Issues in Cybersecu- rity Education	Morris Worm	One of the first computer worms distributed via the Internet and resulted in the first felony conviction in the United States under the 1986 Computer Fraud and Abuse Act
Cybersecurity and Society	HP Face- Tracking Web- cams	HPs webcam failed to track the face of a black man and an explanation on the reasons why
Professional Responsibility in Cybersecurity Research & Industry	Randal Schwartz	The case of State of Oregon vs. Randal Schwartz, which deals with the compromised computer security during this time as a system administrator for Intel
Responsible Disclosure	St. Jude Medi- cal Security Dis- closure	The case of vulnerabilities found in an implantable cardiac devices manufactured by St. Jude Medical which impacted companies stock prices as well as patient safety
Whistleblower, Leaker & In- sider Threat	Shadow Brokers	A hacker group who publishes several leaks containing hacking tools from the NSA
Law & Ethics	The Need for a Computer Crime Innocence Project	The cases of Julie Ameroo and Michael Fiola in which digital forensic evidence was misrepresented
Privacy	Apple FBI De- bate over Encryp- tion	Dispute the concerns whether and to what extent courts in the United States can compel manufactures to assist in unlocking cryptographically protected data

Table 4: The case studies and descriptions of the course.

How essential was this course topic?

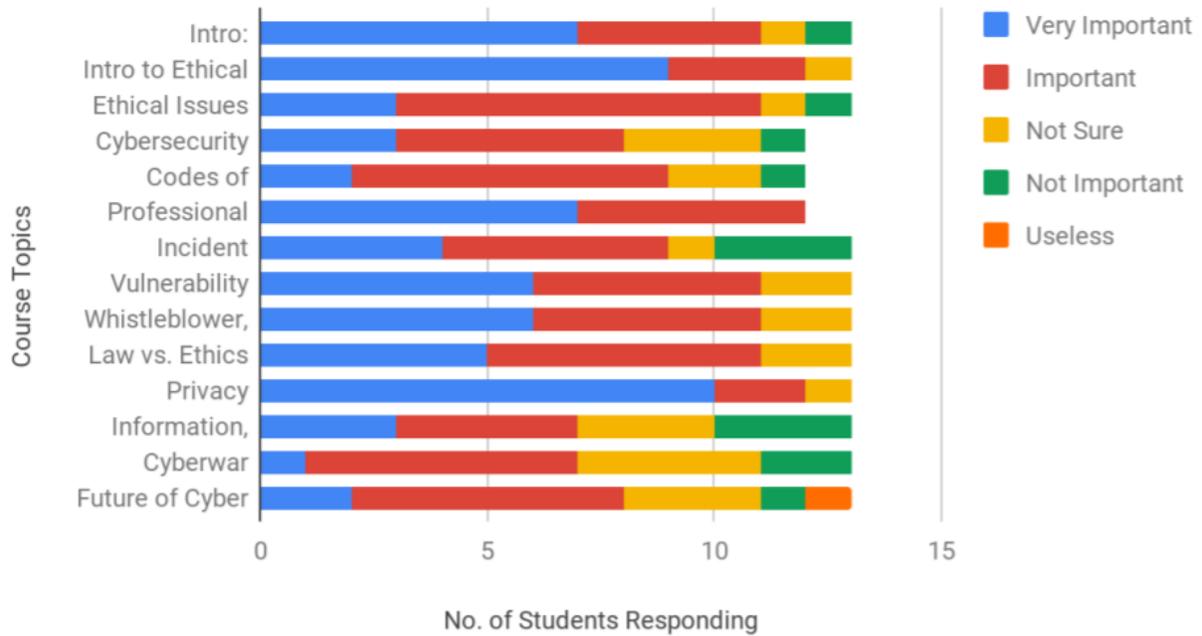


Figure 1: The survey results for: How Essential was this Course Topic?

To What Extent Did This Course:	
increase your awareness about the ethical dilemmas in cybersecurity?	4.36/5
increase your awareness of your own ethical intuitions?	3.93/5
increase your critical reasoning skills?	3.78/5
increase your collaborative problem solving skills?	3.07/5
increase your professional judgement of ethical issues?	3.64/5
facilitate a culture of dialogue?	4.93/5

Table 5: The survey results on course learning objectives

Rated Difficulty of Each Topic

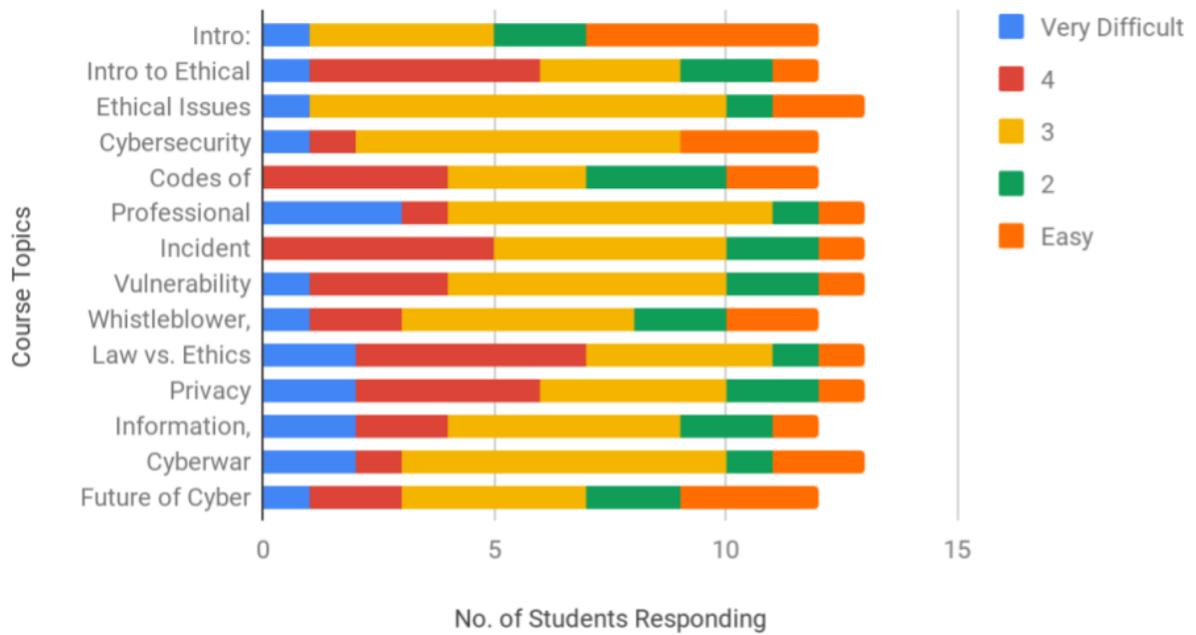


Figure 2: The survey results for: Rated Difficulty Level of Each Topic

When Each Topic Should be Covered

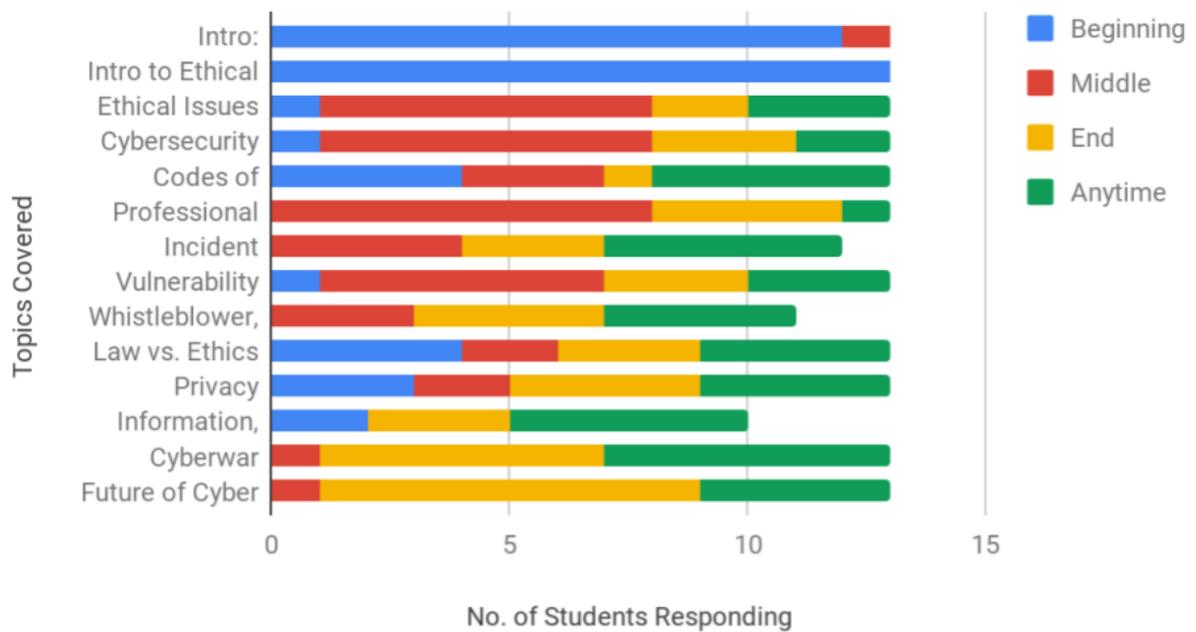


Figure 3: The survey results for: When Each Topic Should Be Covered