Cybersecurity Ethics Education: On "Future-Proofing" the Education We Provide

In this idea paper, I propose a kind of ethics education for cybersecurity that I believe is needed if we are to have any hope of "future-proofing" the education we provide. Cybersecurity education equips students to take profound action in the world and at the same time positions them to operate in a space in which the rules are often ill-defined. The field of cybersecurity is far from establishing codified standards of ethics and the few laws we do have in this area lag woefully behind the speed of technological innovation. We must recognize that we are educating the decision makers of tomorrow who will play a significant role in shaping the future of society. Amidst the rush to prepare a generation of cybersecurity professionals, this requires that we develop long term educational innovations that can prepare tomorrow's thought leaders for the unknown and uncertain futures before them.

Although it is encouraging that the NICE Cybersecurity Workforce Framework and the CAE Knowledge Units, two of the major curricular guidelines for cybersecurity, address ethics in cybersecurity, they both rely on a rule- and compliance-based approach to ethics education. The NICE 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.[1] Similarly, included among the CAE Core Knowledge Units is: Policy, Legal, Ethics and Compliance. This knowledge unit intends "to provide students with an understanding of information assurance in context of the rules and guidelines that control them," by having students list and describe applicable laws and policies, which includes responsibilities for handling vulnerabilities.[2]

While knowledge of relevant laws and policies are an important place to begin, I believe that a rule- and compliance-based approach to ethics education is insufficient for cybersecurity. I briefly offer two reasons for this, here. First, because our laws cannot keep up with the speed of technological innovation. A preeminent example supporting this claim is the chief law we have for regulating cyberspace, the 1986 Computer Fraud and Abuse Act (CFAA), which, according to Josephinne Wolff's recent analysis of five cases, struggles to

[1] Newhouse, William, Stephanie Keith, Benjamin Scribner, and Greg Witte. "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework." *NIST Special Publication* 800 (2017): 181, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

[2] CAE Community, "Policy, Legal, Ethics and Compliance," Core Knowledge Units (2018). https://www.caecommunity.org/resources/ku-cards/ku/policy-legal-ethics-and-compliance.

> 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.[3]

We are preparing students to operate in a realm that is not yet well contained by laws, standards, and norms. We need to recognize this by preparing students to not only have knowledge of yesterday's rules and laws, but to also be able to envision and establish the norms, rules, and policies of tomorrow.

Second, I draw on the educational philosophy of John Dewey in claiming that an ethics education of direct instruction in following the rules only amounts to something "in the degree to which pupils happen to be already animated by a sympathetic and dignified regard for the sentiments of others. Without such a regard, it has no more influence on character than information about the mountains of Asia."[4] A student's own inclinations and prior beliefs play a significant role in determining their ethical conduct. Cybersecurity ethics education must recognize this and find innovative ways to draw upon students' own ethical inclinations. Dewey continues, maintaining that within a democratic society, to attempt to get reliable results through an ethics education of direct instruction is "to rely upon sentimental magic."[5] There is an irony here in that ostensively, we are endeavoring to develop a cybersecurity workforce in order to uphold our democratic society. Yet, in the case of cybersecurity ethics education, I suggest that we not only need to educate *for* democracy, but *through* it as well.

I conclude by proposing an alternative approach to cybersecurity ethics education that involves creating intentional space for engaging in a cumulative and ongoing process of ethical inquiry. 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. The aim of this alternative approach is to foster a kind of ethical culture that can endure in the face of uncertainty and ever-emerging potentialities.

---

[3] Wolff, Josephine Wolff, "The Hacking Law that Can't Hack It," *Slate* (2016), http://www.slate.com/articles/technology/future_tense/2016/09/the_computer_fraud_and_abuse_act_turns_30_years_old.html.

[4] John Dewey, *Democracy and Education*, New York: The Free Press (1916), 354.

[5] Ibid.

Jane Blanken-Webb is a Postdoctoral Research Associate at the Information Trust Institute at the University of Illinois at Urbana-Champaign, where she is taking the lead as co-principal investigator on a grant funded initiative, Ethical Thinking in Cyber Space (EThiCS), supported by the National Security Agency. The main aim of this grant is to develop and teach a cybersecurity ethics curriculum, which was piloted during the Spring semester of 2018. She holds a PhD specializing in Philosophy of Education from the University of Illinois at Urbana-Champaign and her work has been published widely in the field of education. In addition to extensive teaching experience at the university level, she has four years of experience teaching in K-12 environments. Jane and has been working in cybersecurity education since the Fall of 2016 and is closely involved with the Illinois Cyber Security Scholars Program, an NSF funded Scholarship for Service program.