Where is the Justice?
What We Don’t Know about Cyber Ethics*

Jennifer Petrie-Wyman

Anthony Rodi

Richard Albert McConnell

Introduction

Due to the pandemic and the rapidly changing cyber situation that society finds itself in today, every walk of life is finding ways to employ Internet solutions to whatever discipline in which they are trying to operate to support social distancing and flattening the curve. In times like this people may hurriedly seek solutions without considering the ethical ramifications. Twitter and Facebook have revolutionized social connection through cyber innovation. Yet the year of 2020 revealed the unanticipated consequences of the misapplication of open-source free- speech cyber platforms. What happens when cyber innovations are misapplied to misinformation campaigns and leveraged to support hate speech and violence? Do we have the right to lie to others in the cyber domain? Should Twitter and Facebook be permitted to de-platform bad actors? Most might agree that we should prevent bad actors in the cyber domain from inciting violence and criminal activity, but we may not understand the specific ramifications of the cyber environment in which these actions are operating. How do we begin to educate citizens on cyber misinformation, virtual hate speech, and ultimately each citizen’s role in fostering ethics in the cyber domain?

Data and how it is managed is becoming increasingly important in this rapidly evolving situation in the cyberspace that may have far reaching consequences to society (White et al., 2019). For example, should an educator conducting a virtual class over the Internet record that class session? Many might say, Why not? Would their answer change if they discovered that

* Note: This article is a shortened version of a conference paper presented in March 2021.

that video recording was backed up on the cloud indefinitely (*Collaborate Ultra—File and Recording Storage FAQ, Behind the Blackboard!*, 2020)? Is it possible that such videos could compromise personally identifiable information (PII) and thus violate the Family Educational Rights and Privacy Act (FERPA) (Hlavac & Easterly, 2015)? If that teacher deletes that recording out of the classroom, is it deleted from the cloud, or does that data become orphaned data? If so, what are the ramifications of orphan data (Shepley, 2016)? What societal problems could result with a lack of trust in our digital systems? What systems, policies, and procedures are we putting into place to prevent damage to digital trust in our society (Lynch et al., 2016)? When capturing and storing data, are we really getting informed consent from those who provide the data when most informed consents are so confusing and often not read, and if read, not understood (Thomson, 2019; Petroni et al., 2016)? Should access to cyber education be limited to those with the highest aptitude or the most money, or do all citizens necessitate foundational cyber knowledge? Policy and lawmakers should grapple with questions like these. Such questions might have been useful in the increasingly less-fictional case of *Jurassic Park* regarding the ethical ramifications of introducing dinosaurs into the modern world (Spielberg, 1993). The above questions indicate there is a gap in the body of knowledge regarding cyber ethics and how data is curated. One of our problems in understanding this gap in knowledge is a lack of ability to understand how we got to this point.

One need only look at the current pandemic to see inequalities in education based on household access to the Internet. The Internet is a system of systems with an economic culture that is complex and potentially confusing for average users (Greenstein, 2020). The reality of inequalities, in terms of access combined with considerable sums of money, could create an environment fertile for unethical behavior to spawn. On the one hand, some might claim there are standards and accepted practices in cyber that would encourage ethical practice; they just need to be enforced in some meaningful way (Brantly, 2016). On the other hand, the Internet continues to evolve in some ways like ungoverned spaces and could cause some to ponder the need for improved programs for studying cyber ethics. Either way, researchers and practitioners should investigate how to apply ethics in this complex environment.

Therefore, the above-discussed Internet realities might suggest the need to address the following problem: The problem encouraging unethical behavior in cyberspace is Perceived Cognitive Distance (PCD), a culture of rationalization that excuses bad acts over cyberspace, a lack of individual and collective accountability, and a lack of cohesive policies governing data curation. New programs promoting ethics education tailored to the unique complexities of cyberspace could potentially address the above problem statement. A new model of cyber ethics leadership may also provide structural solutions to this problem.

The Current Cyber Ethics Leadership Gap

In 2021, it will be thirty years since the world wide web became publicly accessible. This cyber revolution triggered large-scale transformations across computer science, communication, social and political structures, economic functions, and individual behaviors (Berners-Lee & Fischetti, 2000). While the world has witnessed tremendous growth in the speed, application, and access to cyber technologies, only over the past ten years have scientists and professionals started to critically examine the outcomes and impact of the cyber use from an empirical perspective on a broad scale (Silfversten et al., 2019a; Yaghmaei et al., 2020a). The concept and function of cyber ethics, cyber ethics education, and cyber ethics leadership has just started to gain momentum across industry experts, policy analysts, educators, and citizen cyber users (Silfversten et al., 2019b; Yaghmaei et al., 2020b).

The COVID-19 global pandemic has further propelled the field of cyber ethics as businesses, organizations, institutions, and schools are quickly adapting to working in a fully virtual world. This virtual waterfall has exposed both our nation's cyber readiness as well as our cyber vulnerabilities, including a deficit in cyber ethics training and inequities in access to cyber technologies (Craig, 2019; Lee, 2019; Yaghmaei et al., 2020b). The Black Lives Matter Movement of 2020 has further unearthed a deficit in cyber leadership rooted in ethics and justice as businesses and tech firms have had to confront their own systemic racism and sexism. This article aims to build synergy on the significance and impact of cyber ethics across sectors, propose a broad-scale leadership change model, and formulate policy recommendations to advance cyber ethics education and leadership in the US with potential application to other countries.

The growing concern for cyber ethics has also accelerated due to an explosion in large- scale cyberattacks, data breaches, and the rise of nation-state hackers interfering with elections and government agencies. The field of cybersecurity has started to incorporate cyber ethics, yet significant gaps in the quality and quantity of cyber ethics training remain across industry, the military, and the education sector. The shortcomings of current cyber ethics educational programs are compounded by the fact the US is confronting a cybersecurity and tech workforce deficit, in which there is a pipeline shortage of qualified job applicants with requisite skills to work in jobs related to cyber defense (*K12 Computer Science Framework*, 2016a). The US is also confronting a shortage of teachers capable of teaching computer science education and the skills necessary to effectively instruct cyber education and cyber ethics education on a broad scale (Gross, 2018; *K12 Computer Science Framework*, 2016b).

The PCD of the cyber domain provides ripe ground for unethical cyber actions. At the same time, this PCD has also perpetuated an insulated tech sector often blind to the inequities in its own workforce. The professional computer science and cybersecurity workforce is disproportionately composed of white males and Asian American males (*K12 Computer Science Framework*, 2016b; Martin et al., 2015). This article examines cyber ethics as fundamentally interconnected to inclusion, equity, and justice.

Recent research findings are yielding significant insights into the need to reconsider and expand our knowledge and application of cyber ethics across multiple sectors (Yaghmaei et al., 2020b). The call to integrate cyber ethics into education and training across sectors is emerging in order to promote digital citizenship, national and global security, democracy, and racial and social justice (Mossberger et al., 2008; Yaghmaei et al., 2020b). Cyber ethics can transform professions and society to be more conscious of cyber threats, privacy, and inequities, which would then encourage the development of cyber solutions that promote justice, equity, and democratic rights.

The Elephant in the Cyber Ethics Room: Cyber Privilege, Inequity, and Justice

From the foundation of computing, inequity has persisted in the cyber workforce. The cyber and Internet revolution promised to democratize our world, creating an interactive global audience, reducing barriers to press and entrepreneurship success, yet the gains of cyber have often benefited a limited group of people, largely white male professionals from middle to high-income backgrounds. In 2015, only 24.7% of those employed in computer and mathematical occupations were female, 8.6% Black or African American, and 6.8% Hispanic or Latino (Greening, 2012; *K12 Computer Science Framework*, 2016b). Similar trends can be observed across gender and historically marginalized populations globally, with white males comprising 92% of the tech developer profession and professionals with white or European descent making up 72% of developers (Kapor Center, 2021; StackOverflow, 2019). Recent tech professionals are beginning to call out this inequity not only in the workforce, but in the design of the technology referring to cyber racial injustice as the "New Jim Code" (Benjamin, 2019). While corporations and higher education institutions are attempting to expand the population of cyber professionals and reconsider biases in algorithms and technology, the impact of these recent interventions has been marginal.

In 2021, only half of the schools in the US offer a substantial stand-alone course in computer science in high school. Students with the least access to computer science courses are African Americans, Hispanics, Native Americans, and students from rural areas (*K12 Computer Science Framework*, 2016b). The COVID-19 pandemic and the Black Lives Matter movement are exposing systemic structures of racism in America, including the severe inequities in access to cyber education. In addition, the pandemic has further exposed the effects of the digital divide, ready access to the Internet, and appropriate productivity tools, such as a laptop or home computer. This technology gap further hinders STEM and cyber ethics education in underserved populations. An infusion of ethics into cyber dialogs and policy debates is pertinent to be able to foster ethical dialogs and create equity and inclusion in cyber education.

Complexity of Environments across Businesses & Institutions in the US

Our world today is a data-driven, technology-enabled, hyper-connected ecosystem connected by the Internet of Things (IoT). We have combined our personal and professional environments with every technology possible to make things more connected, convenient, and interoperable. We benefit from the reach of the Internet, the volume of collected big data, and the sheer power of emerging technologies, if accessible. As a result, we have also created not only a dependency on technology, but incredible vulnerabilities to these ecosystems. Greengard reinforces this issue in his 2019 article, "What makes the IoT so powerful—and so dangerous— is the fact that devices and data now interconnect across vast ecosystems of sensors, chips, devices, machines, and software. This makes it possible to control and manipulate systems in ways that were never intended" (Greengard, 2019). As the rapid pace of technology and threats has expanded, leaders across sectors remain underprepared and under-educated in what is needed to combat cyber threats and inequities. Cyber ethics knowledge remains in isolated silos of IT specialists and cyber security professions, leaving leaders across sectors and citizens at large underprepared to confront cyber threats.

Our current environment during the COVID-19 pandemic consists of a very large percentage of the workforce working remotely from home in makeshift offices on personal networks. Teachers are conducting online and remote instruction for the first time using many tools with little to no training. The Boston Consulting Group (BCG) conducted a study in March 2020 on remote work with a focus on cyber security. They estimated about "30 million people are working from home in the US and over 300 million worldwide," using varying technologies including personal mobile phone and computers. Without good training and security protocols, many of these remote workers may fall victim to social engineering, phishing schemes, and cyberattacks, as Coden Et al cautions, "Cyberattacks are like the COVID-19 virus itself. Patching your systems is like washing your hands. And not clicking on phishing emails is like not touching your face," (Coden, et al, 2020).

Systemic Injustice and Constricted Leadership in Cyber Ethics Education

The roots of cyber ethics leadership deficits circulate back to a faulty pipeline of cyber ethics education and pervasive inequities in access to computer science education. Following World War II, computer science rapidly accelerated, yet only a select group of professionals and leaders participated in the creation of this new industry (Curtis, 2012; O'Regan, 2016; Reilly, 2003). As computer science graduate degree programs expanded in the 1970s and 1980s, the students enrolling in these courses remained comprised predominately of white males from middle to high-income backgrounds. These select computer scientists, as well as a small group of philosophers and science fiction writers, were among the first to consider the ethical ramifications of computer science technology. For example, Isaac Asimov's three laws of robotics continues to influence cyberlaw and ethics (Asimov, 1950). The application of ethics to the field of computer science also began to be debated among policy experts (Curtis, 2012). Yet, in the early years of the computer age, morals and ethics were primarily debated on the periphery. Leadership placed greater attention to competitive advantage and technological innovation in the Cold War landscape over ethical and justice implications.

The birth of the personal computer (PC) created an expansion in computer science courses and a slight growth in ethical considerations and policies governing computer use. From the onset, access to computers in American public schools was highly skewed to high-income districts, with low-income districts facing limited resources for computers (Kirby et al., 1990).

Throughout the 1990s, US computer science education expanded in K-12 schools. School districts began to (1) offer computer science courses across K-12, (2) build computer labs for all students to access, and (3) create specialized programs for gifted and talented students. While the numbers of computers per student increased as a result of additional Title I funds, schools faced a deficit in teachers with the skills to actually instruct computing. In 1996, only fifteen percent of teachers had received nine hours of instruction in educational technology (Parker & Davey, 2014). Through gifted and talented programs, some school districts acquired advanced computing technology, such as robotics and coding software, and could train small groups of students in advanced computing. Instructors of gifted and talented programs could receive specialized training or draw on university programs offering high school outreach. The extent to which cyber ethics was considered in these new educational programs is marginally covered in literature. Additionally, there is limited literature on the experience and outcomes of computer science education as a field because states did not have explicit computer science standards for K–12 until recently (Tilley-Coulson, 2016). Computer science content is often imbedded in math and science standards, making assessment challenging (Tatnall & Davey, 2014). In 2016, only five states had independent computer science standards and by 2019, thirty-four states had adopted computer science standards with mixed degrees of implementation (Education, 2019; Tilley-Coulson, 2016).

Even as access standardized computer science education grows, persistent inequities remain. As of 2015, only five percent of US high school students enroll in the AP Computer Science course and only fifty percent of students have access to a computer science course, with low-income school districts in rural and urban populations being disadvantaged (*K12 Computer Science Framework*, 2016b). Complicating the implementation of quality of computer science courses is the evidence that the majority of superintendents, principals, teachers, students, and parents are unable to differentiate between computer literacy (typing and being able to use basic computer functions) and computer science (Wang & Ravitz, 2016). In another survey, pre-service teachers were not prepared to model or teach cyber ethics, cyber security, and cyber safety due to limited knowledge of subjects and could only model four percent of the skills needed to instruct cyber ethics, cyber security, and cyber safety. The report illuminated the advanced skills required to ensure cyber security in the classroom. The effect of limited computer science education and inadequate cyber ethics training for students results in most students becoming passive users of technology and a marginal number of students become interactive critical users of computing technology or creators of cyber content. This lack of understanding about the mechanisms, function, and critical use of cyber technologies makes American citizens especially vulnerable to malicious cyber threats.

Shortfalls in Current Cyber Leadership: The Integrative Cyber Skills Model

Over the past decade, cyber leaders witnessed the exponential rise in digital technology spurred by the rapid adoption of smart devices. The precipitous change left leaders across industry and educational sectors at a loss on how to train workers and educate students on digital technology. Often students and junior colleagues demonstrated higher cyber competencies than their teachers and supervisors/leaders. With few models to draw on, a reactive leadership approach ensued, with leaders across sectors adopting an integrative cyber skills education strategy across industry and subjects with cyber skills being learned in relation to job-function or subject-function vs. a comprehensive competency approach. Examples of integrated cyber skills in the K-12 and higher education classroom include (1) online software to organize and deliver course content, (2) social media, (3) real time and recorded video, (4) instant access to film, music, speeches, and lectures, (5) digital course material, (6) instant access to digital data, and (7) ability to connect quickly with students via email and chat for course questions (Cambridge Assessment International Education, 2017). The rationale for the adoption of integrative cyber education has been due to (1) the rapid integration of technology into almost all disciplines and careers and (2) the limited availability of advanced computer science resources and teachers (Education, 2019; *K12 Computer Science Framework*, 2016b).

The integration of cyber into the curriculum has helped to facilitate a growth in (1) collaborative and social learning, (2) interdisciplinary learning, (3) accessible and adaptive learning. Additionally, researchers are beginning to notice positive effects on student learning in classes facilitated with digital technology compared to traditional classrooms including (1) positive influence on learning motivation, (2) increased intercultural and global knowledge, (3) an increase in interdisciplinary learning (Lin & Chen, 2017; Tiven & Fuchs, 2018). It should also be acknowledged that large-scale evaluation of the effects of digital and cyber education is an emerging field, and some studies have reported mixed results and negative learning outcomes including (1) a decrease in attention, (2) a decrease in writing and reading, (3) an increase in cyberbullying, and (4) an emphasis on quantitative content at the expense of the arts and the humanities (OECD, 2019; Rodideal, 2018; Taylor, 2012). More research is required to determine the effectiveness and outcomes of digital learning, particularly when the classroom moves to a fully online format as was the case during the global COVID-19 pandemic.

While the integrative approach has provided an immediate adoption of technology in the workplace and classroom, the critical and ethical use of technology has been marginally considered. There is wide consensus that an integrative computer science curriculum is not enough for the long-term needs of the future work force (Gross, 2018). In addition to integrating digital technologies, organizations and educators are advocating for the need to adopt computer science education, which includes cyber ethics more broadly as a discipline unto itself to support the advancement of graduates that can be creators of cyber content rather than only cyber users (*K12 Computer Science Framework*, 2016b). Additionally, there is a strong demand from educators to increase the research and assessment on cyber ethics education to determine most effective models and training (Oslejsek et al., 2020).

As advanced cyber education is often introduced only in specialized programs at the undergraduate and graduate level, professional training in cybersecurity and information technology has emerged as way to educate workers on the job on cyber technologies and protect against cyber threats. Additionally, tech firms, as well as the National Security Administration, certain government agencies, and the US Department of Defense offer their own comprehensive skills training to specifically address the cyber security needs of their organization's own workforce (US Cyber Command, 2020).

Reconsidering Cyber Ethics Paradigms

Over the past decade the field of cyber ethics has emerged alongside the expansion of the cybersecurity and the tech industry. Several news events have also pushed the topic of cyber ethics to the forefront of national attention including (1) the disclosure of the US drone warfare program (2) the Facebook–Cambridge Data Analytica scandal, (3) Russian interference in the US elections, (4) the misinformation campaigns populating Twitter and Facebook during the 2020 election and post-election period, among many more. Case analysis of these cyber events alongside emerging research into the ethics of cybersecurity, data and computer use, cyberlaw, and racial and social justice has promoted the emergence of new constructs and paradigms to investigate and evaluate cyber ethics. The events of 2020 laid bare the need to critically reexamine ethical values consideration in the cyber context. Enduring justice paradigms, such as truth, freedom of speech, and democratic leadership oaths have confronted uncharted cyber terrain that ultimately demand a need to reconsider what justice and ethics mean in the cyber domain.

The Constructing Alliance for Value-Driven Cyber Security recently published a report analyzing the ethical values being discussed in current cyber ethics research—see Table 2 for a summary of common ethical paradigms (Yaghmaei et al., 2020b). These data-driven ethical values demonstrate both the depth and significance of cyber ethics in cybersecurity and across industries as we enter the 2020s. While these values and ethical dilemmas are starting to be researched, marginal literature exists about the best practices for incorporating these ethical values and dilemmas into instruction and training for professionals and students (Yaghmaei et al., 2020b). Critically examining the ethical values considerations is pertinent, as the year of 2020 has left practitioners, researchers, and citizens with more questions than answers to cyber ethics dilemmas. An important initial aim is visualizing how these ethical paradigms might interact with values in the field of cyber ethics, especially in relation to the challenges described in the problem statement above. Specifically, how might PCD, rationalization of bad acts over cyber space, lack of individual and collective accountability, and a lack of cohesive policies governing data curation influence ethical paradigms and cyber values? (see Table 1 and Figure 2).

Table 1. Industry Most Common Ethical Paradigms (Yaghmaei et al., 2020b).

This table was adapted from the Yaghmaei er al.'s Constructing an Alliance for Value-Driven Cyber Security (CANVAS) Report (2020), with the authors developing the ethical value considerations for the education industry.

Industry	Ethical Value Considerations	Cyber Example
Health	Non-Maleficence/ Beneficence ↔ Safety	Do no harm online
	Privacy ↔ Security	Unauthorized access
	Trust ↔ Confidentiality	Patient health records
	Autonomy ↔ Consent	Decisions about their health data
	Equality ↔ Accessibility	Unequal treatment due to degree of digital literacy
	Fairness ↔ Justice	Hidden costs of technology
Business	Security Breaches ↔ Confidentiality	Lost data threat to privacy
	Security, Transparency, & Control	Third party data use
	Security, Compliance, Costs & Benefits	Does everyone follow data security?
	Access, Privacy, & Data Integrity	Hackers promoting free flow of information
	Security, Profit, & Data Accuracy	Offshore/ Outsource and data security concerns
	Consent & Trust	Surveillance
	Security, Acceptability, & Usability	Internet use code of conduct
National Security	Accessibility ↔ Security	Not trained to protect self/nation online
	Legality ↔ Safety/Security	Laws slow to respond to new technology
	Privacy/ Protection of Data ↔ Security	Individual vs. state security
	Confidentiality ↔ Trust	Fake Russian Facebook accounts spreading disinformation eroding public trust in news
	Connectedness ↔ Equity of Access	Consumer/ producer equity of access
	Accessibility ↔ Prosperity	Internet as public service
	Interconnectivity ↔ Security	Digital Blueprint of troops
	Cyber Awareness ↔ Security	Rapid technological change

Industry	Ethical Value Considerations	Cyber Example
Education	Autonomy ↔ Consent	Rights of child vs. legal guardian
	Interconnectivity ↔ Security	Recording videos vs. disclosing data of minors
	Equality ↔ Accessibility	Disparities in access to the Internet across socio-economic status
	Cyber Awareness ↔ Security	Rapid technology change and lack of teacher preparation
	Legality ↔ Safety/Security	Who is responsible for the child in a virtual classroom?
	Privacy/ Protection of Data ↔ Security	Third party providers of e-learning, i.e. Blackboard, Canvas, Google Classroom, etc. Need to relook definitions for Education records and Personally Identifiable Information (PII) For Example, currently video recordings of classes are not considered Education records or PII.

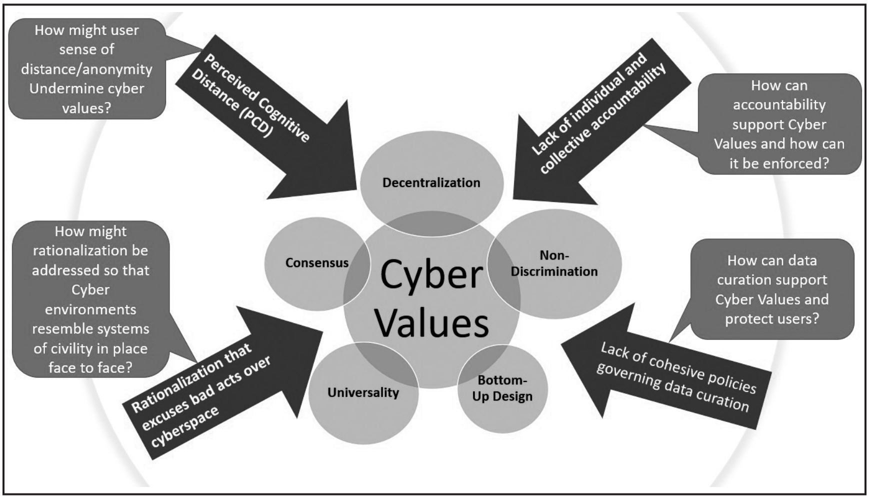

How might user sense of distance/anonymity Undermine cyber values?
Perceived Cognitive Distance (PCD)
Lack of individual and collective accountability
How can accountability support Cyber Values and how can it be enforced?
Decentralization
Consensus
Cyber Values
Non-Discrimination
How might rationalization be addressed so that Cyber environments resemble systems of civility in place face to face?
How can data curation support Cyber Values and protect users?
Rationalization that excuses bad acts over cyberspace
Universality
Bottom-Up Design
Lack of cohesive policies governing data curation

Figure 2. Cyber values and their challenges

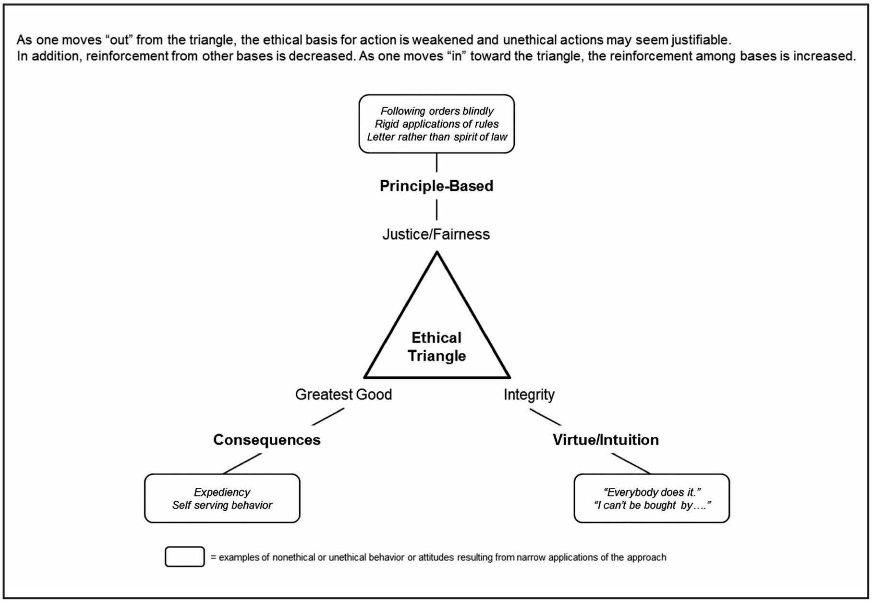

As one moves "out" from the triangle, the ethical basis for action is weakened and unethical actions may seem justifiable.
In addition, reinforcement from other bases is decreased. As one moves "in" toward the triangle, the reinforcement among bases is increased.
Following orders blindly
Rigid applications of rules
Letter rather than spirit of law
Principle-Based
Justice/Fairness
Ethical Triangle
Greatest Good
Integrity
Consequences
Virtue/Intuition
Expediency
Self serving behavior
"Everybody does it."
"I can't be bought by…."
= examples of nonethical or unethical behavior or attitudes resulting from narrow applications of the approach

Figure 3. The Ethical Triangle (Svara, 2011)

Ethics Theory

There are three specific areas of ethics theory that could be useful in improving ethics in cyberspace. Those ethical theories include but are not limited to virtue, principles, and consequences (Pojman, L. & Fieser, J., 2006; McConnell & Westgate, 2019). For example, individuals motivated to do the right thing and live the good life might be impelled by virtue ethics to prevent unfair practices in cyberspace. Those who believe that the accepted practices and norms of the Internet along with laws governing its use would discourage cybercrime and cyber bullying may be using principle-based ethics. Finally, individuals who encourage the application of fair practices and equal access to the Internet because it is best for everyone involved might be using consequence-based ethics. Ultimately, to improve cyber ethics education, theorists and practitioners should engage in a discussion of combining all three of these approaches to ensure thoughtful and ethical practices and policies (See figure 3, Svara, 2011). Such a scholarly discussion would be greatly beneficial in the field of cyber where ethics education is a knowledge gap crying out to be filled.

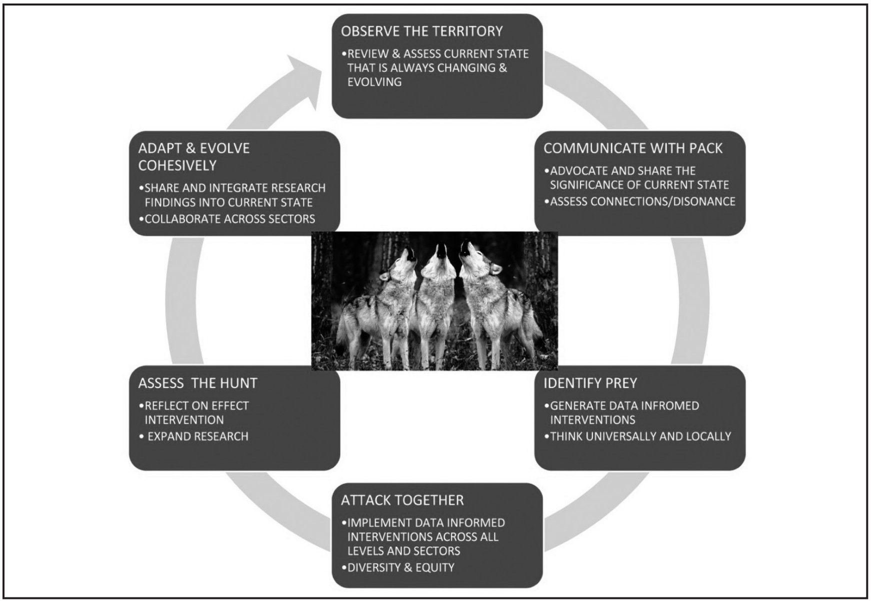

OBSERVE THE TERRITORY
•REVIEW & ASSESS CURRENT STATE THAT IS ALWAYS CHANGING & EVOLVING
COMMUNICATE WITH PACK
•ADVOCATE AND SHARE THE SIGNIFICANCE OF CURRENT STATE
•ASSESS CONNECTIONS/DISONANCE
IDENTIFY PREY
•GENERATE DATA INFROMED INTERVENTIONS
•THINK UNIVERSALLY AND LOCALLY
ATTACK TOGETHER
•IMPLEMENT DATA INFORMED INTERVENTIONS ACROSS ALL LEVELS AND SECTORS
•DIVERSITY & EQUITY
ASSESS THE HUNT
•REFLECT ON EFFECT INTERVENTION
• EXPAND RESEARCH
ADAPT & EVOLVE COHESIVELY
•SHARE AND INTEGRATE RESEARCH FINDINGS INTO CURRENT STATE
•COLLABORATE ACROSS SECTORS

Figure 4. The Wolf-Trap Change Model. Image provided via public domain (Jooinn, 2020).

Creating & Implementing a National Cyber Ethics Leadership Change Model

In response to the current limitations in cyber ethics education in the US and the increasing pace and scale of cyber threats and attacks, a national cyber ethics leadership change model is urgently needed. Rather than a specific set of standards for different sectors and/or disciplines, the authors propose a broad-scale change model to be adopted and adapted across educational, business, and military institutions. This model draws structure from three change models: (1) Lewis's Unfreeze, Change, Refreeze model, (2) Kolb's learning cycle of concrete experience, reflective observation, abstract conceptualization, and active experimentation, and (3) Deming's change cycle of Act, Plan, Check, Do.

The six-step process described above in the Wolf-Trap Model has three core functions (1) to implement agile and adaptive cyber ethics education, (2) to promote universal cyber ethics education that is responsive to distinct needs of the industry or location, and (3) to build a research infrastructure to advance cyber ethics education and strengthen national security (See figure 3, Wolf-Trap Change Model). This model aims to create a national cyberethics leadership and education paradigm that is continuously adaptive to changing conditions, as the state of technological advancement in the cyber sector is constantly advancing. The model also emphasizes the importance of creating a template that is agile to local conditions yet interconnected as the threat from unethical cyber behavior can affect wide systems including public infrastructure, software, and apps used by millions of people. The model also prioritizes the need to assess, conduct research, and revaluate as the field of cyber ethics is emerging with limited resources currently available.

The first step of this model, "Observe the Territory," calls for the review of the current state of cyber ethics. This article is a first attempt at reviewing the state of data and cyber ethics broadly in the US, and this step calls for the development of additional reviews and observations across sectors and geographic contexts. Each wolf has a different perspective of the territory, and each of these viewpoints contributes to the development of a more accurate and cohesive strategy. An inclusive critical reflection of how we got to the point of wide-scale unethical behavior and systemic injustices in the cyber domain is a pertinent first aim for leadership striving to change and reform.

The second step of this model, "Communicate with the Pack," calls for the development of network infrastructure to develop and share information across sectors and disciplines. As cyber ethics is an emerging field, current information of cyber ethics is often trapped in disciplinary silos, which if shared can contribute informed interventions on a broad scale. This second step also identifies that there is public need to develop data and cyber ethics awareness for all citizens, as cyber behavior and threats have the potential to affect each of us, not just trained informational technology professionals. Cyber ethics is a national security consideration due to the scale of its impact on every user. The perspective of each wolf is useless to the pack if it is not communicated effectively.

The third step of this model, "Identify the Prey," focuses on the critical need to connect the style and scope of cyber ethics education interventions to the specific needs of the sector and current state. This step emphasizes the need to proactively design interventions to reduce unethical behavior. The prey is conceptualized as the gaps in our educational system that make us vulnerable to external and internal cyber threats. If we do not address and confront our own "prey" i.e., citizens needing wide-scale cyber ethics training, another predator will jump on our "prey" before we have any time to react. If we fail to intervene, our enemies force us into a reactive posture vs. proactive. Wolves who cannot identify the prey accurately and quickly may unexpectedly find themselves becoming the prey. There is also significant demand to frame racial and social injustice as an essential prey in the cyber ethics domain.

The fourth step of this model, "Attack Together," calls for the need to have data and cyber ethics educational interventions across all sectors and industries, including public institutions, for-profit companies, non-profit organizations, and the military. While each sector may have a different approach, each player—each wolf—should support the overarching mission to enhance cyber ethics education for all. Implementing interventions to reach all citizens across all socio-economic divisions is paramount. Diversity and inclusion are emphasized in this step, as systemic racism and sexism has created inequities in cyber education in the US that we still must challenge. Wolves instinctively know that for any attack to be successful, it must be coordinated, synchronized, and employ the appropriate number of wolves at the decisive point to trap the prey.

The fifth step of this model, "Assess the Hunt," draws from Kolb's learning model in which behavior transformation requires critical reflection, observation, and analysis. This step of the model also calls for the need to develop a research infrastructure specifically attuned to analyzing the effectiveness of cyber ethics educational interventions especially longitudinally, as the authors in-depth literature review found few studies reporting the empirical effects of cyber ethics education. Wolves must learn from their experience during the hunt and apply those lessons to future attempts to trap their prey.

The sixth step of the model "Adapt and Evolve Cohesively," emphasizes the interconnected nature of cyber threats and the need to share and integrate research findings across sectors. This step calls for developing networks, conferences, and policies that crosses sectors. There is pertinent need to strengthen and connect the needs of professional sectors with educational institutions to address the critical and timely needs of industry that is always changing and evolving. This step focuses on advancing national security by integrating and learning from the needs and research outcomes of professionals across sectors. This step brings home the foundational need of cyber ethics education to have a broad and universal mission that is informed from diverse perspectives. Wolves are more effective at countering threats when they stay in their packs, mass their power decisively, and adapt more effectively and quicker than their prey.

A Wolf-Trap Change Model Case Study

A short case study on applying the Wolf-Trap change model to improving cyber ethical behavior in virtual business school team projects, shows how the model builds critical, inclusive, and broad-change for business students on the topic of cyber ethics.

In the first step of the model, "Observe the Territory," the faculty of a business school course is asked to critically review how their current students are behaving in terms of cyber ethics. The faculty member starts the course off with an anonymous survey asking students to talk about their experience working on teams virtually and if they have encountered bad behavior, such as virtual lies, harassment, or discrimination. Students are also asked to comment on their own use of cyber technologies and social media and to identify challenges and dilemmas. By including the perspective of all students, the faculty member hopes to get a broader view of the problem-territory.

In the second step of this model, "Communicate with the Pack," the faculty member designs three learning assignments to broaden students perspectives and networks on cyber ethics, (1) the professor gives a presentation and guided discussion on business cyber ethics and virtual teams introducing students broadly to the topic domain, (2) students participate in a group project where they learn about resources for building inclusive virtual teams, and (3) students are asked to interview a business leader who is working to promote cyber ethics in the workplace and share their findings with the course. By having students look broadly at the topic of cyber ethics, students will learn ways to communicate about the topic of cyber ethics across sectors and in the workplace. Students are also asked to develop inclusive virtual ground rules for their team project that will happen throughout the semester, to try to ensure that students are actively behaving ethically throughout the course as the course is delivered online.

In the third step of this model, "Identify the Prey," the faculty member has the entire class determine a broad cyber ethics problem statement that they want to work on throughout the semester, which they determine is the need to create inclusive cyber ethics programs. Each group then identifies a specific cyber ethics intervention to work on with their teams as their semester project. One group of students focuses on addressing the cyber disparities in a local low-income school. Another group works on examining the issue of discriminatory cyber harassment happening in their university. And a third group partners with a local organization to work on creating inclusive social media platforms to confront the challenges of the 2020 social media misinformation campaigns.

In the fourth step of this model, "Attack Together," the student teams work independently on a common problem statement throughout the semester but share their group project outcomes with the entire class in a final presentation and class-wide discussion. It is important that the student groups come back together to learn the ways other students were working on the cyber ethics challenge.

In the fifth step of this model, "Assess the Hunt," each student completes a reflective assignment on the outcomes of their group intervention and identifies strengths, weaknesses, opportunities, and threats to future work on cyber ethics. Students also share out their reflections in student groups to learn about the different perspective each student has on the project experience.

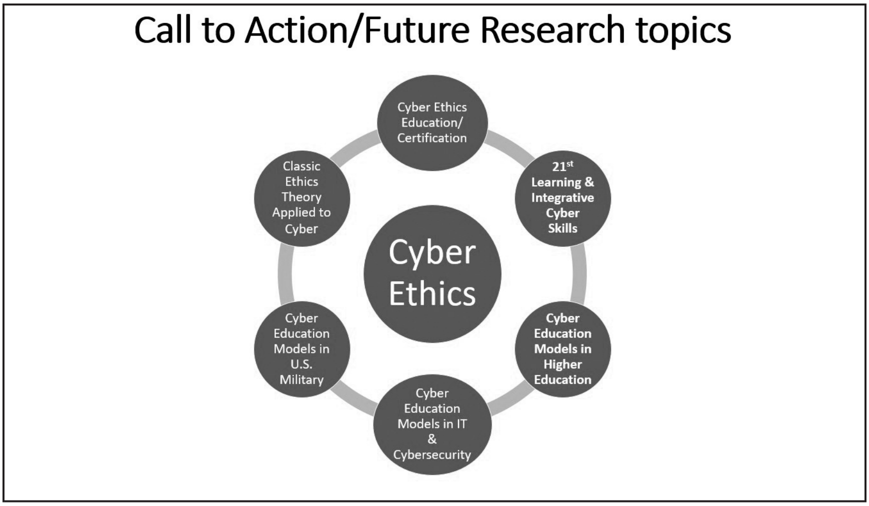
In the sixth step of the model "Adapt and Evolve Cohesively," the faculty member invites the student teams to participate in a school-wide virtual conference on cyber ethics where students share out their project outcomes and also learn from a broader university community about developments happening in cyber ethics. The virtual conference serves to teach students the value of continuous learning and adaption as a broad community of students and professionals.

The Leading Role Higher Education & Military Can Play in Implementing a Cyber Ethics Leadership Change Model

An interdisciplinary and inter-industry approach to cyber ethics leadership and education is required as the impact of cyber threats and cyberattacks is broadly impacting businesses, organizations, public sectors, and individual users. Both higher education institutions and the US military are in a unique position to serve as thought leaders in developing innovative and interdisciplinary cyber ethics education in the US. Universities maintain expertise broadly across information systems, computer science, business, law, public health, public policy, and education. The US military often has the most current and pertinent cyber technology and cyber security resources to protect our national security. The collaborative expertise of both higher education and the US military has the potential to deploy cyber ethics training to students and professionals broadly. This educational and ethics reflection process is especially pertinent today as the US military continues to investigate new uses of cyber platforms that could have far-reaching ethical ramifications. For example, over the last decade, US military intelligence collectors have attempted to capture biometric data (fingerprints, iris scans, and facial scans) from eighty percent of the population of Afghanistan (Jacobsen, 2021; Talbott, 2021). Since it is a war zone, few have reflected on how to curate such data. Who uses, stores, and deletes such data? Since such technological applications have made their appearance in the US, perhaps it is time to determine how this data is captured, used, and stored as well as who controls the delete key. This is a clear example of how much of a struggle it can be to keep up with the ethical ramifications of cyber. This is a key example of runaway developments in cyber the ethical ramifications of which we are struggling to keep up.

A Call to Action & Recommendation

In 2021, the world has never been more virtually interconnected. This accelerated access to cyber has allowed businesses and institutions to adapt and continue to function in the face of an unprecedented global pandemic, requiring citizens to social distance and work and learn from home on a massive scale. While this seamless connectivity has been a blessing, it has also diguised a grim reality. The forced embrace of the remote environment along with the necessary complementary technologies has created a noticeable gap in the digital divide among poorer school districts and underserved populations, causing even greater cyber awareness risks. As a collective, we don't understand the cyber and data systems we use daily, nor their ethical consequences. Rather than maintain this status quo, this article calls attention and urgency to intervene through the development of increased education, research, and theory and model building on cyber and data ethics. The US is underprepared to ethically handle the pace and scale of our data and cyber use. Now is the time to heed Ian Malcolm's warning given in *Jurassic Park* about the risks of using an unknown technology that brings dinosaurs back to life without understanding the consequences of that technology. Now is the time to investigate, study, and train ourselves to be more critical and ethical cyber users before we experience an unintended consequence or cyberattack or cyber-instigated violence that leaves us incapable of rebooting.



Call to Action/Future Research topics

Cyber Ethics

Cyber Ethics Education/ Certification

21st Learning & Integrative Cyber Skills

Cyber Education Models in Higher Education

Cyber Education Models in IT & Cybersecurity

Cyber Education Models in U.S. Military

Classic Ethics Theory Applied to Cyber

Figure 5. Call to Action/Future Research Topics

References

Asimov, I. (1950). *I, Robot*. Spectra.

Benjamin, R. (2019). *Race After Technology*. Polity Press.

Berners-Lee, T., & Fischetti, M. (2000). Weaving the Web: The Orginial Design and Ultimate Destiny of the World Wide Web. Harper Business.

Brantly, A. F. (2016). The Most Governed Ungoverned Space: Legal and Policy Constraints on Military Operations in Cyberspace. *SAIS Review of International Affairs*, *36*(2), 29–39. https://doi.org/10.1353

Cambridge Assessment International Education. (2017). Digital technologies in the classroom. Collaborate Ultra—File and Recording Storage FAQ. (2020, July 2). https://blackboard.secure.force.com/publickbarticleview?id=kA770000000CbqL

Craig, R. (2019, November). Closing the Cybersecurity skills gap. *Forbes2*.

Curtis, R. (2012). Computer Science Education Past and Radical Changes for Future. In T. Greening (Ed.), *Computer Science Education in the 21st Century* (19–27). Springer.

Education, C. S. (2019). *State of Computer Science Education Equity and Diversity*. Greening, T. (Ed.). (2012). *Computer Science Education in the 21st Century*. Springer.

Greenstein, S. (2020). The basic economics of Internet infrastructure. *Journal of Economic Perspectives*, *34*(2), 192–214. https://doi.org/10.1257/jep.34.2.192.

Gross, A. (2018). Survey Large Gap Between Demand for Computer Science, Schools Actually Teaching It. 1–3.

Hlavac, G. C. Esq., & Easterly, E. J. Esq. (2015, April 1). *FERPA Primer: The Basics and Beyond*. National Association of Colleges and Employers (NACE). https://www.naceweb.org/public-policy-and-legal/legal-issues/ferpa-primer-the-basics-and-beyond/.

Jacobsen, A. (2021). First Platoon: A Story of Modern War in the Age of Identity Dominance (1st Edition). Dutton.

K12 Computer Science Framework. (2016a). https://doi.org/10.1017/CBO9781107415324.004

K12 Computer Science Framework. (2016b). https://doi.org/10.1017/CBO9781107415324.004.

Kirby, P., Oescher, J., Wilson, D., & Smith-Gratto, K. (1990). Computers In Schools: A New Source of Inequity. *Computers Education*, *14*(6), 537–541.

Lee, T. (2019, November). How to close the tech skills gap. *Scientific America*.

Lin, M., & Chen, H. (2017). *A Study of the Effects of Digital Learning on Learning Motivation and Learning Outcome*. *8223*(7), 3553–3564. https://doi.org/10.12973/eurasia.2017.00744a.

Lynch, H., Bartley, R., Metcalf, J., Petroni, M., Ahuja, A., & David, S. L. (2016). *Building digital trust: The role of data ethics in the digital age*. Causeit, Inc. https://www.causeit.org/data-ethics.

Martin, A., McAlear, F., & Scott, A. (2015). *Path not found Disparities in Access to*. *1*(0), 1–16.

McConnell, R., & Westgate, E. (2019). What were you thinking: Discovering your moral philosophy using the forensic approach. *The International Journal of Ethical Leadership*, *6* (Fall 2019), 60–78.

Mossberger, K., Tolbert, C. J., & McNeal, R. S. (2008). *Digital Citizenship: The Internet, Society, and Participation*. MIT Press.

O'Regan, G. (2016). Introduction to the History of Computing. Springer.

Oslejsek, R., Rusnak, V., Burska, K., Svabensky, V., Vykopal, J., & Cegan, J. (2020). Conceptual Model of Visual Analytics for Hands-on Cybersecurity Training. *IEE*. Transactions on Visualization and Computer Graphics, 2626(c), 1–1. https://doi.org/10.1109/tvcg.2020.2977336.

Parker, K., & Davey, B. (2014). Computers in Schools in the USA: A Social History. In A. Tatnall & B. Davey (Eds.), *Reflections on the History of Computers in Education* (pp. 203–211). Springer.

Petroni, M., Long, J., Tiell, S., Lynch, H., & David, S. L. (2016). *Data Ethics: Informed Consent and Data in Motion*. Causeit, Inc. https://www.causeit.org/data-ethics

Pojman, L. & Fieser, J. (2006). *Ethics: Discovering Right and Wrong* (7th ed.). Cengage Learning.

Reilly, E. D. (2003). Milestones in Computer Science and Information Technology. Greenwood Press.

Shepley, J. (2016, April 29). *Ignoring Orphaned Data is a Risky Business*. CMSWire.Com. https://www.cmswire.com/information-management/ignoring-orphaned-data-is-a-risky-business/.

Silfversten, E., Frinking, E., Ryan, N., & Favaro, M. (2019a). Cybersecurity: A State-of-the-art Review. In *RAND Europe*. http://hdl.handle.net/20.500.12832/2423

Silfversten, E., Frinking, E., Ryan, N., & Favaro, M. (2019b). Cybersecurity: A State-of-the-art Review. In *RAND Europe*. http://hdl.handle.net/20.500.12832/2423.

Spielberg, S. (1993). *Jurassic Park* [Drama/Adventure]. Universal Pictures.

Svara, J. (2011). Combating corruption, encouraging ethics: A practical guide to management ethics. Rowman and Littlefield Publishers Inc.

Talbott, C. (2021, February 11). 'First Platoon,' featuring a Washington state soldier, details U.S. military's troubling quest for 'identity dominance.' *The Seattle Times*. https://www.seattletimes.com/entertainment/books/first-platoon-featuring-a-washington-state-soldier-details-u-s-militarys-troubling-quest-for-identity-dominance/.

Tatnall, A., & Davey, B. (Eds.). (2014). Reflections on the History of Computers in Education. Springer.

Thomson, J. (2019, July 1). *Ethics In The Digital Age: Protect Others' Data As You Would Your Own*. Forbes. https://www.forbes.com/sites/jeffthomson/2019/07/01/ethics-in-the-digital-age-protect-others-data-as-you-would-your-own/.

Tilley-Coulson, E. (2016). National Association of State Boards of Education States Move toward Computer Science Standards. *National Association of State Boards of Education*, *23*(17).

Tiven, B. M. B., & Fuchs, E. R. (2018). Evaluating Global Digital Education: Student Outcomes Framework.

Wang, J., & Ravitz, J. (2016). Landscape of K-12 Computer Science Education in the U. S.: Perceptions, Access, and Barriers. *SIGCSE '16: Proceedings of the 47th ACM Technical Symposium on Computing Science Education*, 645–650.

White, G., Ariyanchandra, T., & White, D. (2019). Big Data, Ethics, and Social Impact Theory – A Conceptual Framework. *The Journal of Management and Engineering Integration*, *12*(1), 9–15.

Yaghmaei, E., Poel, I. van de, Christen, M., Gordjin, B., Kleine, N., Loi, M., Morgan, G., & Weber, K. (2020). *White Paper 1 Cybersecurity and Ethics* (Issue 700540).