WHY SHOULD I BEHAVE?
ADDRESSING UNETHICAL CYBER BEHAVIOR THROUGH EDUCATION

Jennifer Petrie-Wyman
University of Pittsburgh

Anthony Rodi
University of Pittsburgh

Richard McConnell
U.S. Army Command and General Staff College

ABSTRACT:

The pace and scale of change within the fields of data and cyber technology are so large that practitioners in these fields are focused on mission accomplishment over reflection on the ethical ramifications of evolving policies and procedures. As a consequence of the COVID-19 global pandemic, practitioners are scrambling to provide services over virtual platforms without pausing to reflect on the ethical implications and moral consequences of their increased virtual behavior. The escalation of data and cyber use without an ethical consciousness of that virtual technology makes us blind to unintended consequences and vulnerable to attacks by perpetrators and nation states exploiting our limitations. This paper examines the pertinent and timely need to reconsider cyber ethics, ethical cyber theories, and the limited and inequitable cyber ethics education happening in the United States. The authors then present a model for creating a comprehensive data and cyber ethics educational model and examine the leading role higher education and the military can play in advancing the model. The paper concludes with a call to collective action by professionals, educators, and leaders in the data and cyber technology sector and presents recommendations.

KEY CONCEPTS:

1. ***Introduction: Strengthening National Security through Cyber Ethics Education***
2. ***Increasing Cyber Threats across Businesses & Institutions in the USA***
3. ***A Review of Cyber Ethics Education in the US***
4. ***Theory of Ethics***
5. ***Creating & Implementing a National Cyber Ethics Education Model***
6. ***The Leading Role Higher Education & Military Can Play in Creating Cyber Ethics Education Model***
7. ***A Call to Action***

INTRODUCTION:

> ***Ian Malcolm:*** Don't you see the danger, John, inherent in what you're doing here? Genetic power is the most awesome force the planet has ever seen and yet you wield it like a kid who has found his dad's gun. … I'll tell you the problem with the scientific power you're using here. It didn't require any discipline to attain it. You read what others had done and you took the next step. You didn't earn the knowledge for yourselves, so you didn't take any responsibility for it. You stood on the shoulders of geniuses to accomplish something as fast as you could, and before you even knew what you had, you patented it, and packaged it, and slapped it on the side of a plastic lunchbox and now you're selling it. ...
>
> ***John Hamond:*** I don't think you're giving us our due credit. Our scientists have done things that nobody has ever done before.
>
> ***Ian Malcolm:*** Yeah but your scientists were so preoccupied with whether they could they never stopped to think if they should (Spielberg, 1993).

The above interaction from the famous film *Jurassic Park* in many ways captions the current situation regarding the rapidly changing cyber situation that society finds itself in today. Due to the pandemic, 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. Should John Hammond create an amusement park filled with dangerous prehistoric predators? An entire series of movies seems to indicate he should not. Should data collected over the Internet be protected? Most might agree that it should but may not understand the specific ramifications of the cyber environment in which they are operating. 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 a teacher

conducting a virtual class over the Internet record that class session? Many might say, why not? Would their answer change if they discovered that 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)? Questions like these are among those with which policy and lawmakers should grapple. There is a gap in the body of knowledge regarding cyber ethics and how data is curated. The purpose of this white paper is to review the current state of data and cyber ethics and suggest areas of research, education, and policy changes that could help fill this gap in the body of knowledge. One of our problems in understanding this gap in knowledge is a lack of ability to understand how we got to this point.

One hundred years ago, the availability of electricity in homes and businesses although present, was not always a commonplace occurrence. Today, most homes in the United States have electricity -- a luxury item one hundred years ago. Numerous studies have been conducted examining the connection of economic growth to the availability of electricity as well as the similarities between the growth of electricity availability and that of the Internet (Kirikkaleli et al., 2018). Scholarly research related to this topic would indicate that societies that lacked electricity and access to the Internet might also be subjected to a higher incidence of poverty and a lack of opportunities. 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 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. What follows is a more detailed discussion of the existing cyber threats we face, the gaps in addressing those threats, and how education in ethics theory and practice can help create a safer future for all of us in cyberspace.

In order to effectively address the topic of unethical behavior in the cyber context, the authors used visualization and design to develop the above problem statement:

Problem statement calculation:

Current State/independent variable: The current cyber climate creates the conditions to encourage unethical behavior due to Perceived Cognitive Distance (PCD), rationalization of bad acts over the cyberspace, decreased individual and collective accountability, and a lack of cohesive policies governing data curation.

Desired outcomes/dependent variable: comprehensive innovations in ethics education across multiple modalities resulting in an adjusted cyberculture that reduces PCD, rationalization of bad acts over the cyberspace, an increase in individual and collective accountability, and protection of users through cohesive policies governing data curation.

Two ways to look at the problem statement:

Question: How can educators address a cyber climate that encourages unethical behavior given Perceived Cognitive Distance (PCD), rationalization culture of bad acts over cyberspace, a lack of individual and collective accountability, and a lack of cohesive policies governing data curation?

Assertion: The problem causing 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.

Essential Definitions

Cyber: Involving the use of computers and digital technology especially through the Internet.

Ethics: The investigation and analysis or moral principles and dilemmas as well as an examination of rules, standards, and guidelines that govern moral behavior by managing a balance of the three points of the ethical triangle: virtues, principles, and consequences (see figure 3, Svara, 2011) .

Cyber Ethics: The investigation and analysis or moral principles and dilemmas as well as an examination of rules, standards, and guidelines that govern behavior in the cyber space and cyber domain. Cyberethics education could mitigate Perceived Cognitive Distance (PCD), the culture of rationalization that excuses bad acts over cyberspace, the lack of individual and collective accountability, and the lack of cohesive policies governing data curation within the cyber domain.

Cyber Domain:

> "A global ever evolving domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers – as well as people, organizations, and processes – which create a dimension of risks, adversaries, and opportunities."(Sobiesk et al., 2015)

Cyber Education: Referring to the instruction of material using cyber technologies as well as the teaching of computer science and cyber technologies. This is a broad term encompassing both the use, application, and creation of cyber technologies. Some experts argue that Moore's law is no longer relevant i.e. the speed of computing is not set to double every two years as had been predicted (Rotman, 2020). That said, the speed of change within the cyber domain still seems to be quite rapid requiring further innovations in educating users on all aspects of operating within that context.

Computer Science Education: "**The study of computers and algorithmic processes, including their principles, their hardware and software designs, their [implementation], and their impact on society**"(*K12 Computer Science Framework*, 2016a; Tucker, 2003).

Virtual Education: "Distance learning conducted in a virtual learning environment with electronic study content designed for self-paced (asynchronous) or live web-conferencing (synchronous) online teaching and tutoring." (Racheva, 2020) Since the beginning of the pandemic, virtual education has increased significantly making this area of inquiry a true growth industry.

Cyber Security: Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information(U.S. Cybersecurity & Infrastructure Security Agency, n.d.)

Cyber Ethics Education: Cyber ethics education encompasses instructing responsible and moral behavior and use of computers and digital technology, critical moral thinking and decision making with cyber and digital technology, as well as technical skills and leaderships and management strategies.

INCREASING CYBER THREATS ACROSS BUSINESSES & INSTITUTIONS IN THE USA

When we think of technology in today's environment, it is difficult to imagine getting through a day without our devices, technologies, social media, or the convenience of the Internet. Even more daunting, is that many of us once lived without any technology.

Our world today is data driven, technology enabled, hyper-connected ecosystems 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. 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).

Every year, we experience an increase of cyber threats, disruptions, and cyber attacks across businesses and institutions in the USA. This explosion of cyber attacks has increased year over year as our environments get more complex and interwoven.

An Explosion in Cyber Attacks & Citizens Unprepared

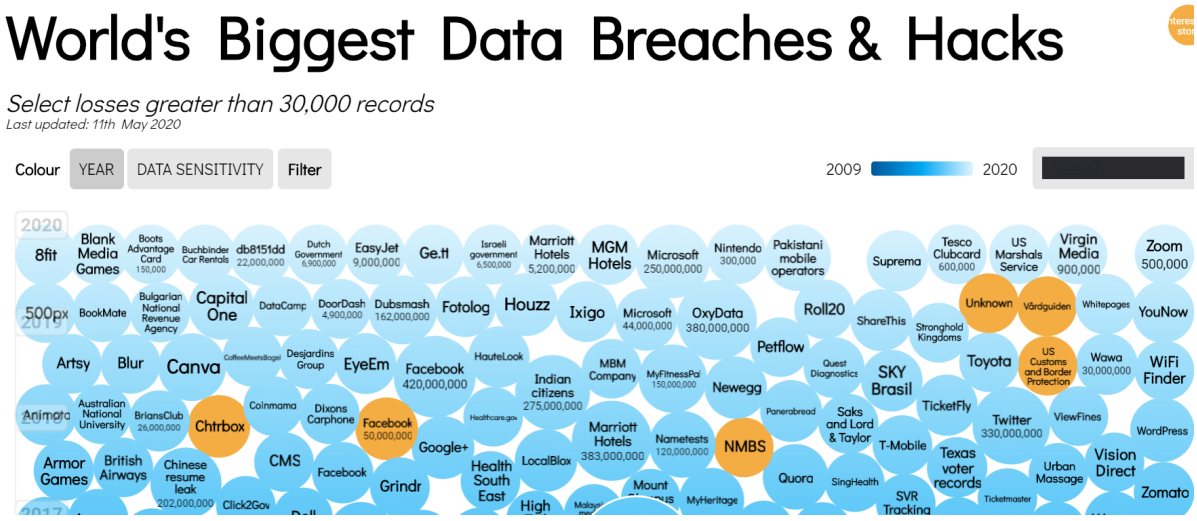
With large scale use of cloud-based servers and integrated big data systems, the incentives of bigger rewards have motivated cyber attackers to continue a record rise in cyber attacks on organizations and governments. The infographic by McCandless, et al., in Figure 1, depicts the rise and severity, year after year, of data breaches.

In his 2019 article, Greengard discusses that

> "Future cybercriminals could take control of a private citizen's refrigerator or lighting system and demand a $1000 ransom in bitcoin in order to restore functionality. It is also not difficult to fathom the threat of a vehicle that won't break, or a pacemaker that stops working due to a hack. Hackers might also weaponize devices and take down financial systems and power grids" (Greengard, 2019, p.20).

Bourdeaux, et al., (2020), expands on the digital environment in their paper as they discuss the rapid evolution of technology-based systems in healthcare, known as "Health Intelligence Systems." The four areas of vulnerability in these systems

FIGURE 1.
World's Biggest Data Breaches and Hacks (McCandless, et al.)



(https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/)

identified as "credential stealing, exploiting unencrypted networks, exploiting software errors, and infiltrating supply chains," provide a huge potential for cyber-attacks, especially during emergency responses and pandemics where multiple governments and global health systems participate in the same "Health Intelligence Systems" (Section 6). This sharing of data and systems creates the ability for a hacker to access multiple databases once access is gained to one database. Healthcare data has become a goldmine for hackers. Davis (2020), has reported that in 2019, according to Protenus Breach Barometer, 41.4 million patient records were breached. As of July 2020, even during the COVID pandemic, the top 10 healthcare data breaches have involved phishing, mishandled patient record disposals and cyber-attacks (para 1).

According to the research conducted by Humayun, et al, (2020), the focus of the study was on the mapping of Cyber Security Threats and Vulnerabilities, as providing from existing research data. The study provided detail around the source of threat and vulnerability of cyber-attacks. Interestingly, of the list of infrastructure targets of the cybercrimes, the following targets that appeared in the top five of the lists: Social media, Mobile Applications, and Networks, are areas that have much human interaction. Within these areas involves human error that is still a common vulnerability. People mistakenly give away information and fall victim to phishing schemes. As a result, training is still a key defense in protection against cyber threats (Humayun, et al.,2020, pp. 3181-3183).

Jaf, et al, (2018), describes key vulnerabilities in the form of insider threats. Organizations can successfully protect infrastructures from outside attacks using key technologies such as firewalls. However, in spite of all of the technologies and strategies used to protect from outside attacks, the biggest risks lie inside of the organization in the form of people. The "Human Factor" in cyber threats, as described by Jaf, et al., as victims of Social Engineering. In our highly technology enabled environments, many non-technical employees have access to critical infrastructures. As a result, it becomes difficult to maintain good security practices and these employees fall victim to attacks (Jaf, et al., 2018, pp. 4987-4989).

Our current environment during the COVID 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 U.S. 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 cyber-attacks. "Cyber-attacks 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).

A REVIEW CYBER ETHICS EDUCATION IN THE US

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, 2000a). 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 and cyber ethics education 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). This article aims to build synergy on the significance and impact of cyber ethics across sectors, propose a broad-scale model of cyber ethics education, and formulate policy recommendations to advance cyber ethics education in the United States.

The growing concern for cyber ethics has also accelerated due to an explosion in large-scale cyber-attacks, data breaches, and the rise of nation-state hackers interfering with elections. 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 is compounded by the fact the United States 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*, 2016b). The U.S. 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*, 2016a).

The Perceived Cognitive Distance (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*, 2016a; Martin et al., 2015). This article examines cyber ethics education as fundamentally interconnected to equity and inclusion.

Recent research findings are yielding significant insights into the need to reconsider and expand our knowledge and application of cyber ethics education 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 security, democracy, and social justice (Mossberger et al., 2008; Yaghmaei et al., 2020b). Cyber ethics education can transform professions and society to be more conscious of cyber threats, privacy, inequities and to develop cyber solutions that promote justice, equity, and democratic rights. To understand the current state of cyber ethics education, the next section highlights important themes in the history of cyber ethics and cyber education. This section reviews literature focusing on cyber ethics, cyber education, and the emerging topic of cyber ethics education.

TABLE 1.
World Wide Web Foundational Ethical Values (World Wide Web Foundation, 2020)

World Wide Web Value	Definition	Application	Challenge to Value
Decentralization	Posting to the world wide web is free from censorship. Permission is not required from a central authority or central controlling node.	The world wide web is created and accessed globally	Authoritative regimes create national firewalls that censor access to individuals, such as China. Manipulative information campaigns by nation states via automated technology "Bots"
Non-Discrimination	Internet service providers must treat all Internet communications equally and not discriminate or charge differently based on type of user, content, equipment, and others.	Net Neutrality critical to keeping the Internet open playing field	Large telecommunications companies dominating the Internet service provider market wanting to offer pay for priority service
Bottom-Up Design	Code available royalty free encouraging maximum participation and experimentation	Library of Common Code, also application of Open Source Data	For Profit Companies/ Hackers
Universality	Common language of code to publish on the Internet regardless of language and geographic location	Program Languages Lisp, C, Perl, PHP, SQL, Java Script	Digital divide, limited literacy in code and language of the Internet
Consensus	For universal standards to work, everyone has to agree to use them	World Wide Web Consortium devoted to open web standards	Censorship threat Criminal activity

The Dawn of Cyber Ethics

When the world wide web was launched, ethics was interwoven into the design and application of the information system, yet many Americans remain unaware of the design and ethical dimensions of the world wide web (Berners-Lee & Fischetti, 2000b). According to a recent Pew research study, the majority of American adults correctly answered less than half of the questions on a digital literacy quiz, demonstrating the need for increase in the quantity and quality of digital education and cyber ethics education (Vogels & Anderson, 2019).

When Sir Tim Berners-Lee, a British computer scientist, created the blueprint for the world wide web in 1989 his design principals were firmly rooted in ethical and democratic values including; (1) decentralization, (2) non-discrimination, (3) bottom-up design, (4) universality, and (5) consensus (Berners-Lee & Fischetti, 2000a; World Wide Web Foundation, 2020). See Table 1 for a description of each world wide web value.

Over the past thirty years, emergent threats and challenges have surfaced to the worldwide web's ethical values impeding the ability of the world wide web to be an application promoting democracy and rights. Cyber hackers, authoritative regimes, and systemic inequities in access to computer science and cyber education have hampered the ability of the world wide web to actualize its foundation to intent to create a more free, open, and democratic world.

Before the world wide web, cyber threats and attacks were frequently performed by computer enthusiasts attempting to experiment and explore the perimeters of the computing (Levy, 2010). Malicious attacks were rare and initial hackers were often commended for their expert computing skills and ability to create positive improvements in computing systems (Levy, 2010). Herbet Zinn, the 17-year old high school dropout the hacked into AT&T's computer system, exemplified the quintessential 1980s hacker as Zinn bragged about his hack and received admiration for it. At the same time, this attacked forced federal authorities to reconcile the importance of how far Zinn penetrated security systems and how close Zinn had come to bringing US telecommunications systems to a complete standstill. Zinn was one of the first hackers to be criminally prosecuted under the Federal Computer Fraud and Abuse Act in 1986 (Middleton, 2017; Goldstein, 2009).

As the world wide web became increasingly integrated across networks and servers, the 1990s saw a growth in malicious hackers seeking to exploit organizations and steel proprietary data for financial gain, yet these hackers were primarily individual computer users. The growth of e-commerce, increased the financial incentive for hackers to launch large-scale attacks on users and organizations prompting an exponential growth in malware and cyber-security firms (Middleton, 2017; Woodrow, 2014). The rise in cyber-bullying, pornography, and illegal commerce escalated in the 2000s prompting a need to consider the ethical dimensions of a free and open communication network, especially in regards to protecting children from explicit content and legal restrictions protecting copyright such as the Napster ruling A & M Records, Inc. vs. Napster (Chibbaro, 2007; GOLDSTEIN, 2003; Ku, 2002).

The Perceived Cognitive Distance (PCD) of the cyber environment allowed for the rise of cybercrime and unethical uses of the Internet throughout its first two decades of use. The expansion of cyber threats and cyber perpetrators to nation-states and cyber-attacks on big data storage systems with data from millions of users has emerged only in the past ten years. The escalation of unethical behavior throughout the Internet's existence remains a pervasive threat to its foundational ethical values.

The Elephant in the Cyber Ethics Room: Cyber Privilege & Inequity

From the foundation of computing, inequity has persisted in 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 of African American, and 6.8% Hispanic or Latino (Greening, 2012; *K12 Computer Science Framework*, 2016a). Recent tech professionals are beginning to call out this inequity not only in the workforce, but in the design of the technology referring to this era 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 2020, only half of the nation's schools offer a substantial stand-alone course in computer science in high school. Students with the least access to a computer science courses are African Americans, Hispanics, Native Americans, and students from rural areas (*K12 Computer Science Framework*, 2016a). The COVID 19 pandemic and Black Lives Matter movement is exposing systemic structures of racism in America, including of the severe inequities in access to cyber education in the U.S. An infusion of ethics into cyber education dialogs and policy debates is pertinent to be able to foster ethical dialogs and create equity and inclusion in cyber.

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 U.S. drone warfare program (2) the Facebook-Cambridge Data Analytica scandal, (3) the Uber sexual harassment scandal, (4) Russian interference in the U.S. elections, among many more. Case-analysis of these cyber events alongside emerging research into the ethics of cybersecurity, data and computer use, and cyberlaw has promoted the emergence of new constructs and paradigms to investigate and evaluate cyber ethics. 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). This report aims to integrate these values into a comprehensive educational model that strengthens workforce knowledge, awareness, and application of cyber technologies. Additionally, it is important to visualize how these paradigms might interact with values in the field of cyber ethics especially in relation to the challenges described in in the problem statement above. Specifically, how might Perceived Cognitive Distance (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 2 and figure 2).

Cyber Ethics Education

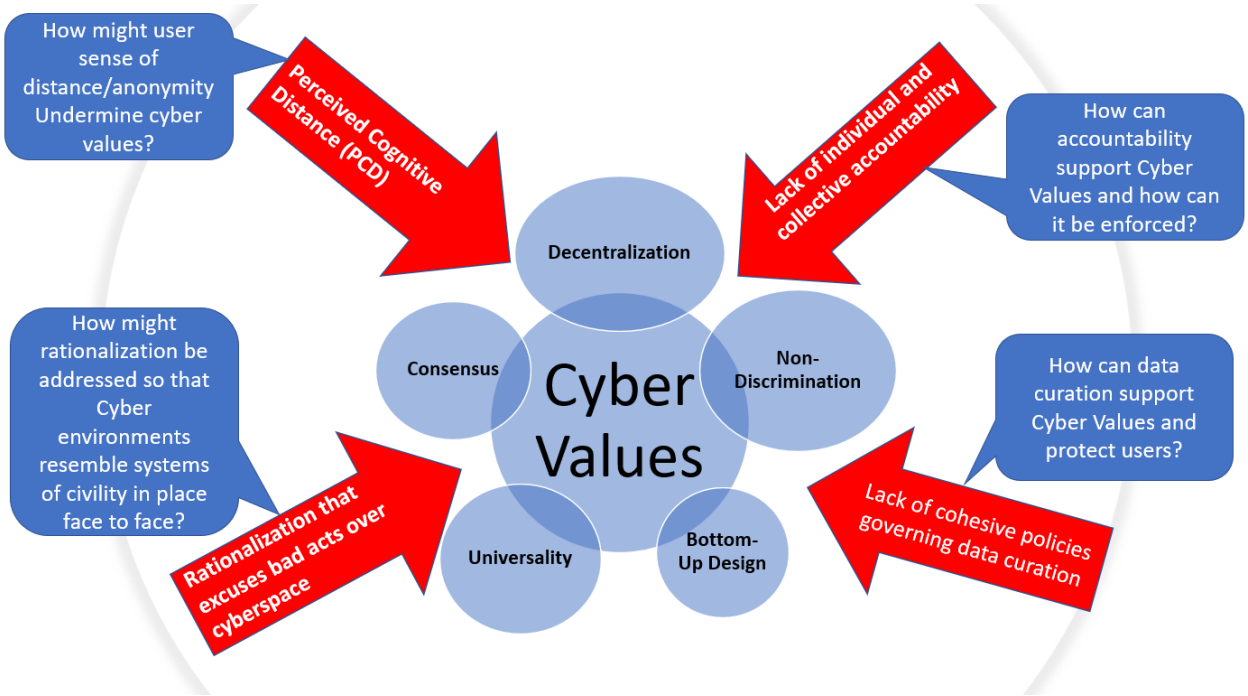
When examining a literature review of cyber ethics education in the United States four general approaches to cyber ethics education emerge: (1) offering courses specific to computer science education in higher education and high school, (2) integrating cyber ethics education into content subjects in higher education and K-12 education, (3) teaching cyber ethics through professional

TABLE 2.
Industry Most Common Ethical Paradigms (Yaghmaei et al., 2020b).
This table was adapted from the Yaghmaei er al.'s 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

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 virtu-al 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 Infor-mation (PII) For Example, currently video recordings of classes are not considered Education rec-ords or PII.

FIGURE 2.
Cyber values and their challenges



training, and (4) teaching cyber ethics through the military and governmental institutions devoted to cyber defense and cyber security.

Computer Science Education & Cyber Ethics in the United States

The initial home for cyber ethics education was in the discipline of computer science, which emerged during the years following World War 2. A select number of higher education institutions, businesses, and the government agencies created computer science labs, such as the Watson Scientific Computing Laboratory founded in 1945 at Columbia University agencies (Curtis, 2012; O'Regan, 2016; Reilly, 2003). 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 robots continues to influence cyberlaw and ethics (Asimov, 1950).

The first U.S. Computer Science Department was formed at Purdue University in 1962 and throughout the 1970s and 1980s computer science graduate degree programs expanded. The students enrolling in these courses were comprised predominately of White males as this was the population of students also majoring in STEM fields at that time. The framing of cyber ethics education throughout the Cold War period often focused on the power of computer science technologies to promote and protect democratic values and defend against computer science technologies used by authoritarian regimes. The application of ethics to the field of computer science and the governance of computer technologies also began to be debated amongst policy experts (Curtis, 2012).

The birth of the personal computer (PC) created an expansion in computer science courses offered at higher education institutions which advanced ethical considerations and policies as the amount of computer users grew rapidly. By the late 1980s, undergraduate courses and K-12 classes started to offer rudimentary computer science education. This education often consisted of a classroom having one computer with students taking turns to have screen time or in computer labs where each student had access to an individual computer for a finite amount of time. Education primarily focused on students learning typing and basic computer functions. 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) The initial instructional mode for computer science class was traditional lecture centered with students following instructor commands and directions on how to operate the computer system and also manage errors, such as learning to select "Save All" before printing to avoid a fatal error that would delete any progress made on your Word document. Entire reports and thesis were lost by forgetting to follow this critical command. In early computer science courses in higher education and K-12, ethics was covered marginally often in conjunction with calls from instructors not to plagiarize, as this was made easier with the "copy-paste" feature, or calls to stop accessing games, like the memorable Oregon Trail, while in the classroom. Ironically, recent educators have pointed out that Oregon Trail actually helped to develop student's ethical decision making as they game made students make critical decisions effecting their family's income, migration, health, and even life, although some have also pointed out that the game reinforced colonial constructs (Charsky and Barbour, 2010; Slater, 2017).

Throughout the 1990s, U.S. computer science education expanded in K-12 schools. School districts began to offer (1) more 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 due to Title I funds, schools faced a deficit in teachers with the skills to actually instruct computing. In 1996, only 15% 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, 34 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 5% of U.S high school students enroll in the AP Computer Science course and only 50% of students have access to a computer science course (*K12 Computer Science Framework*, 2016a). 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 4% 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 ethic 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.

Rise of 21st Learning and Integrative Cyber Skills in the United States

Parallel to schools offering explicit computer science courses, an integrative cyber skills education strategy has also evolved. For the past two decades, K-12 education and higher education institutions have expanded the integration of learning computing and cyber skills through the core curriculum (Code.org, 2 C.E.). The rationale for the adoption of integrative cyber teaching methods, especially at the primary levels, has been due to the (1) the integration of technology into almost all disciplines and careers and (2) the limited availability of advanced of computer science resources and teachers (Education, 2019; *K12 Computer Science Framework*, 2016a).

The integration of cyber education into K-12 and higher education curriculum has created an exponential growth in experience-based learning pedagogies, creative project based learning, and diverse, personalized education, and global interactive learning across the Web. Examples of digital technology use in the everyday 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) course material, (6) instant access to data, and (7) ability to connect quickly with students via email and chat for course questions (Cambridge Assessment International Education, 2017). In 2019, the state of PA, following the wave of other state policy advances,

adopted state-wide standards for computer science that integrated cyber skills into K-12 classroom formally(CSTA K–12 Computer Science Standards - Revised 2017, 2017).

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) 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) decrease in attention, (2) decrease in writing and reading, (3) an increase in cyber-bullying, 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 (Silfversten et al., 2019a).

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 in the classroom, organizations and educators are advocating for the need to adopt computer science education, that 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*, 2016a). 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)

Cyber Ethics Education Program Models

As cyber ethics education is an emerging field, limited large-scale studies examine effective cyber ethics education programs. This section examines current model curriculums and model educational programs emerging in the field of cyber ethics education through case-studies, curriculums, and some emergent empirical studies.

Models in K-12 Education

Digital Citizenship: The CODE.ORG and Computer Science Teaching Association advocate for the inclusion of digital citizenship content throughout their computer science standards throughout the K-12 level. Digital citizenship focuses on teaching students the application and effect of digital technologies on society including politics and the economy. The content knowledge pertaining to cyber ethics is integrated into the entire K-12 curriculum. A challenge to implementing the digital citizenship topics is that there are limited teacher training resources available to teach this content. While CODE.Com offers free training in digital citizenship education for K-8 teachers, the high school training focuses on the technical skills of computer science and does not offer an explicit focus of digital citizenship or cyber ethics (Code.org, 2017; *K12 Computer Science Framework*, 2016b).

Cyber Ethics in Computer Science Courses: Some computer science cover cyber ethics curriculum as cyber ethics is often covered in state computer science standards. As the adoption of state standards is recent for many states, there is marginal data about the quantity and quality of this coverage. The AP computer science course also includes cyber ethics in two or ten units with the subtopics of "Ethical and Social Implications of Computing" and "Ethical Issues around Data Collection" (College Board, 2020)

Cyber Ethics and Moral Development: School curriculums integrate cyber and ethics education with Kohlberg's model of moral development, an age-specific approach to ethical education recognizing that student's behavior and attitude grow throughout their lifetime. Curriculums would focus on increasing awareness of the morals and ethics of cyber including appropriate use of technology, acceptable cyber behavior, how cyber use impacts our behavior, and the interaction of morals in cyberspace (Lewandowski, 2002). This Learning model can be integrated across subject disciplines.

Anti-Cyber Bullying Campaigns: This approach to cyber ethics introduces K-12 students to topics of cyber ethics through the content of cyber-bullying, which adversely impacts adolescents. Cyber-bullying is used a starting point for broader discussions on the use of ethics and digital technologies (Lee, 2016).

Adaptive Cyber Ethics/ Against a Cyber-Tooth Curriculum: This model calls for an adaptive and integrated cyber curriculum to meet the needs of changing technologies and an increasingly globalized world. Critical 21st century learning skills and digital skills are not enough to meet the future needs of students. Cyber-curriculum should emphasize creativity, invention, and global citizenship to create a curriculum that is more flexible and less in need of revision every five years (Higgins, 2014).

Cyber Outreach & Enrichment Programs: Out of the classroom educational programs have emerged in the past decade as a way to diversify and expand equity in cyber ethics education. Programs such as Black Girls Code, Teens Exploring Technology, Hidden Genius Project, and Yes We Code, offer computer science education programs to students at no cost in school districts with limited computer science offerings (Martin et al., 2015)

Cyber Camps: Summer camps that offer intensive cyber education experiences to high school students. One example of a cyber camp is the University of Pittsburgh Institute for Cyber Law, Policy, and Security offers a free week-long Air Force Association Cyber camp for high school students that focus on technical skills, cyber ethics, and systems security. The camp also works towards increasing diversity of students interested in cyber security and STEM education (University of Pittsburgh, 2020).

High School Hackathon: Hackathons have emerged in high schools as a way to collaboratively work on cyber innovations. During a short period of time, student teams are expected to create a solution to an existing problem using technology. Not only do students use computer skills in an interactive format, but they often learn ethical cyber skills, such as following competition cyber rules, maintaining respectful and collegial communication with their team and competitors, and considering the use and consequences of their technology (Hack Pennsylvania, 2019; Major League Hacking, 2020).

Models in Higher Education

Foundational Skills: Traditional approaches to cyber ethics education focus on understanding the ethical theory and skills needed to work ethically and effectively in cyber fields (Beveridge, 2019). Traditionally, these skills are instructed through didactic teaching.

Problem Based Learning: This approach to cyber ethics education focuses on students solving an ethical problem or dilemma by applying research, theory, and practice (Beveridge, 2019). A common approach to teaching problems-based learning is the case-study method, in which the students examine specific real world or fictional cyber ethics dilemmas or threats and articulate their solution to confronting the problem. This approach is common in Business School curriculums instructing cyber ethics.

Experience Based Learning: This educational model incorporates hands-on experience and the practical application of skills in real-world replicated environments, such as in labs, cyber simulation exercises, and out of the classroom experiences such as internships or study abroad. Kolb's model for experiential learning emphasizes a reflective continuum of learning through a four-stage cycle that includes concrete experience, reflective observation, abstract conceptualization, and active experimentation (Beveridge, 2019). Experience based learning with reflective training also allows for students and trainees to connect the content to their own lives and experience, which increases their responsiveness to the instructional material (He & Zhang, 2019)

Cyber Ethics Embedded into the Cybersecurity Master's Program or Undergraduate Program: Cyber ethics is covered as a core course in cybersecurity programs focusing on the policy, law, ethics, and compliance. Of the 37 AACSB accredited Business Schools, 19 programs offered specific cyber ethics courses and also covered cyber ethics throughout other courses such as organizational management (Yang, 2019). The National Initiative for Cybersecurity Education (NICE) also encourages the inclusion of ethics throughout cyber security educational programs (NICE, 2020).

NSA Driven Model: This model establishes cyber ethics education into 2 year and 4 year cybersecurity education programs in the U.S. supporting the national needs of cybersecurity workforce and promote national security. The NSA Model mandates specific course requirements covering cyber policy, law, ethics, and compliance and also organizes courses around adaptive knowledge units vs. foundational courses to allow for an integrative approach to learning (Conklin et al., 2014). The NSA also designates and supports universities as Centers of Academic Excellence in Cyber Operations and Centers of Academic Excellence in Cyber Defense that meet their criteria

Network Ethics Education: Information ethics education is not enough, students require an interactive networks ethics education to understand the ways cyber influences social behavior vs. individual user behavior(Ueno & Maruyama, 2011).

College Hackathons: Hackathons have emerged as a popular form of learning through competition across colleges and universities. Students work with collaborative team members to solve a problem with technology. Colleges and universities offer specialized hackathons related to certain topics, involve students majoring outside of computer-science, and offer hackathons to certain groups of students, such as women-only. Cyber ethics is emphasized throughout the competitions as students must follow certain competition rules and guidelines and debate the use and consequences of certain technological innovations.

Cyber Defense Competition: College students compete in a simulated real world environment to manage and protect a network infrastructure. Technical skills, management skills, and cyber ethics skills are essential to the collaborative teamwork. Students learn through experience the importance of compliance with laws and regulations as well as the application of morals, ethics, and social responsibility to cyber security (Woszczynski & Green, 2017). Woszczynski and Green (2017) emphasized the need to integrate learning outcomes into the design of cyber defense education to strengthen the educational experience for competitors and to link the learning outcomes to skills required in cybersecurity professions.

Cyber Ethics Training for Teacher Education: Cyber-ethics education should be integrated into teacher-training programs to instruct teachers on the cyber-ethics dimensions for students and as teachers. Approaches to instruction include character education covering the ways in which cyber impacts psychology, moral behavior, and empathy*Whitter*. Additional scholars call for teacher training programs to focus on cyber ethics, cyber security, and cyber privacy as an integrative approach to strengthening cyber ethics education in the classroom (Pruitt-Mentle & Pusey, 2010; Pusey & Sadera, 2011).

Professional Cyber Education Models in IT & Cybersecurity

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 and certain government agencies, offer their own comprehensive skills training to specifically address the cyber security and cyber ethics needs of their organizations own workforce. Marginal large-scale empirical data exists on the effectiveness of these professional cyber

education training as the profession is still emerging. Case studies, curriculums, and national discussion about effective cyber training are starting to emerge and the following models of professional cyber training are gaining traction.

Integrated Cybersecurity Training: This model of cyber ethic education calls for cyber ethics education to be integrated into worker performance at all levels. The traditional approach of training specialists is insufficient for the broad scale of cyber threats that exist in institutions and organizations. Cyber ethics training should be required for all employees, with specific training tailored to specific management levels (Gupta et al., 2018). An integrated strategy will allow employees across all levels to have effective communication about cyber safety and security. The Cybersecurity Awareness Training Model CATRAM is a case study example of a firm in Canada that targets cybersecurity training to specific personnel: Board of Directors, Managers, End-Users, and IT staff (Sabillon et al., 2019). Gupta, Bajramovic, Hoppe, and Ciriello also provide an integrative cybersecurity model for nuclear power plants and critical infrastructure (Gupta et al., 2018).

Evidence Based Cyber Ethics Training: As the field of cyber ethics education has limited empirical studies on the effectiveness of cyber ethics training, especially the quantitative outcomes, professionals are arguing for more training programs to be built based on evidence of effectiveness. For example, one of the first large scale studies on information cyber security training found that educational time, the proportion of management training, and outsourcing training each had a meaningful negative effect on the number of security incidents in the organization(Kweon et al., 2019).

Including both Cyber Defense and Cyber Offense Education: As our national cyber security threats continue to grow, there is a need to increase cyber offensive education as most current cyber security programs focus on defensive operations. As more nation-states continue to mount offensive cyber-attacks, this educational model focuses on the need to train highly skilled professionals that can act as key players in cyberspace supporting American interest through offensive operations (Dawson, 2020). The ethical risks of teaching offensive skills are still being debated by military and civilian programs.

Visual Analytics and Cyber Security Simulations: To strengthen cyber security simulations, visual analytics can be integrated into the training platform to support the sensemaking and awareness of participants engagement in the cyber training. The visual analytics process allows students and teachers to incorporate insight and feedback that provides a simple summative score, which is common in hands-on simulations (Oslejsek et al., 2020). The reflective process of visual analytics allows students to create in-depth connections with the training material and potentially have stronger learning outcomes.

Automated Hands-On Training: In order to streamline the operational process of setting-up and managing cybersecurity training, professionals are advocating for automatic training that reduce the entry barrier costs. The automated training CyTrone incorporates interactive and customizable features allowing for user-specific learning experiences (Beuran et al., 2018).

Interactive & Engaging Cybersecurity Training: For cyber-security training focused on increasing employee responsiveness, educational models include making training fun, hands-on, interactive, and personalized as well as considering implementing systems of rewards and positive reinforcement for compliance (He & Zhang, 2019)

High-Fidelity Clinical Simulations: Cyber-security training is integrated into the clinical training of medical professionals through high-fidelity simulations involving real-life scenarios, patient actors, and supervisors to recognize, treat, and prevent patient harm due to cyber-security threats (Dameff et al., 2019). The relevancy of this training model is critical to the healthcare sector as a pilot study on the high-fidelity clinical simulation revealed no participants could recognize the cyber threat, as one physician noted, "Assessment of the technology we use is not even on my radar (Dameff et al., 2019)."

Cyber Education Models in the US Military

Similar to the case of professional cyber educational models, the U.S. military offers its own specialized training in cyber for its service members. Created in 2009, the U.S. Cyber Command serves as the unifying cyber command force for the Department of Defense with its mission "to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners." In addition to the specialization of U.S. Cyber Command, cyber skills are integrated across all eleven unifying commands of the U.S. Department of Defense. While cyber skills training is integrated and implemented across the DoD, the focus of cyber ethics education and cyber ethics training is still emerging. The following educational models are used across the U.S. military (U.S. Cyber Command, 2020).

Models in the US Military

Centralized Training at U.S. Cyber Command: The U.S. Cyber Command serves as a centralized leader in cyber education and cybersecurity training for the DoD offering advanced and integrated training cyber defense and cyber offense including certification standards (U.S. Cyber Command, 2020).

Cyber Education in Basic Training: Starting in 2011, basic training included cyber education with attention to the fundamentals of cybersecurity and cyber-threats (Corrin, 2011).

Special Cyber Education Training is Service Academies: Within the past decade, the U.S. Service Academies have offered majors focusing in cyber education, such as cyber security network, ICT, and computer science. The service academies are also exploring additional ways to expand cyber education beyond technical specialists, such as a requiring a cybersecurity

fundamentals course, expanding cybersecurity electives, incorporating interdisciplinary capstone courses that include cybersecurity, and expanding extra -curricular offerings related to cybersecurity (Spidalieri and McArdle, 2016).

Cyber Ethics Integrated into Advanced Training: Throughout the U.S. military cyber ethics has been integrated into advanced training for military leaders with varying models of adoption and implementation.

Way Forward

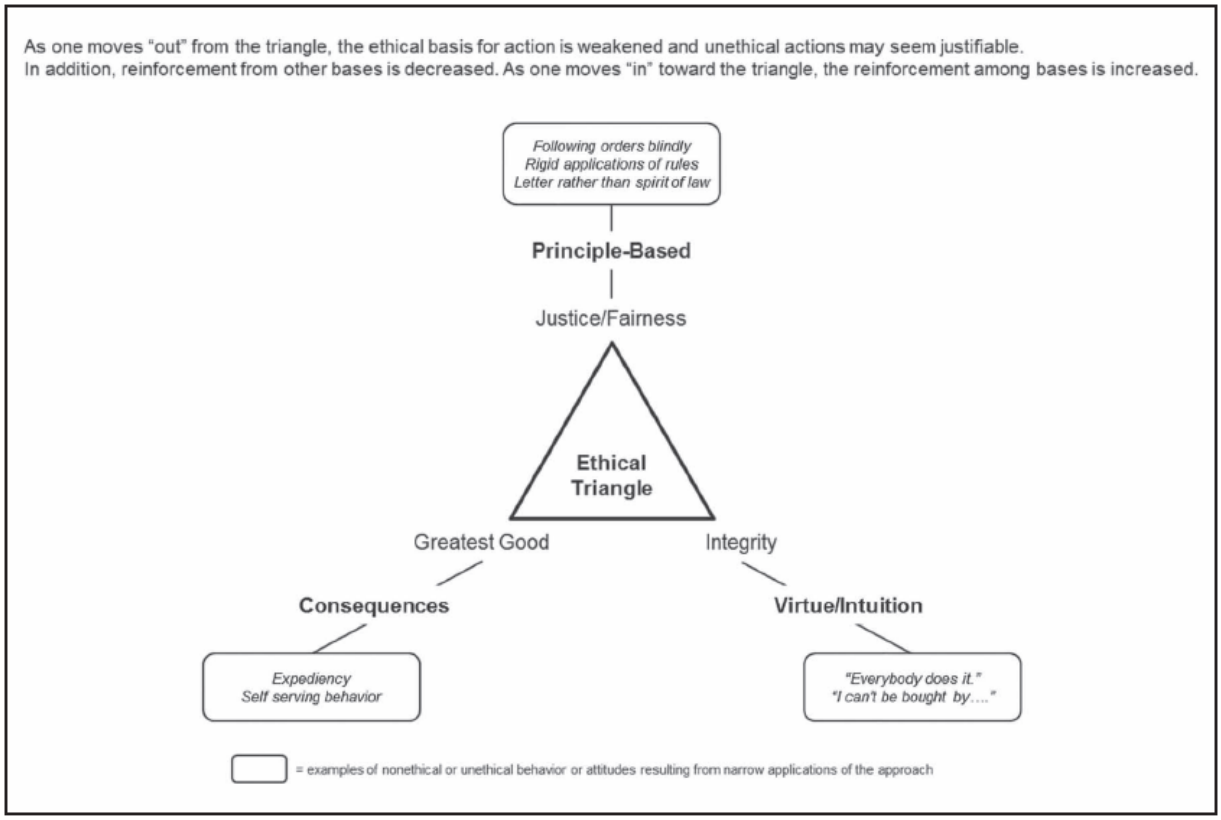
Cyber ethics education is critical to US national security. The increase in cyber engagement in our nation's workforce alongside intensifying cyber-attacks, makes our society, businesses, and institutions vulnerable. The escalating cyber threat demands a broad investment in not only cyber skills training in our workforce, but also cyber ethics education.

Cyber ethics education encompasses instructing responsible behavior and use of computers and digital technology, critical thinking and decision making with digital technology, as well as leadership and management strategies to protect against, disclose, and find solutions to cyber threats and cyber-attacks. While the start of the twenty-first century, emphasized the value of STEM education, the future workforce demands a more critical and comprehensive instruction in cyber technology as our use of cyber technology pervades in our work and daily living. Cyber ethics education can provide an important intervention allowing our workforce to be prepared to prevent, encounter, and remedy cyber threats and also engage in a more humane and civil digital world.

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 principal-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.

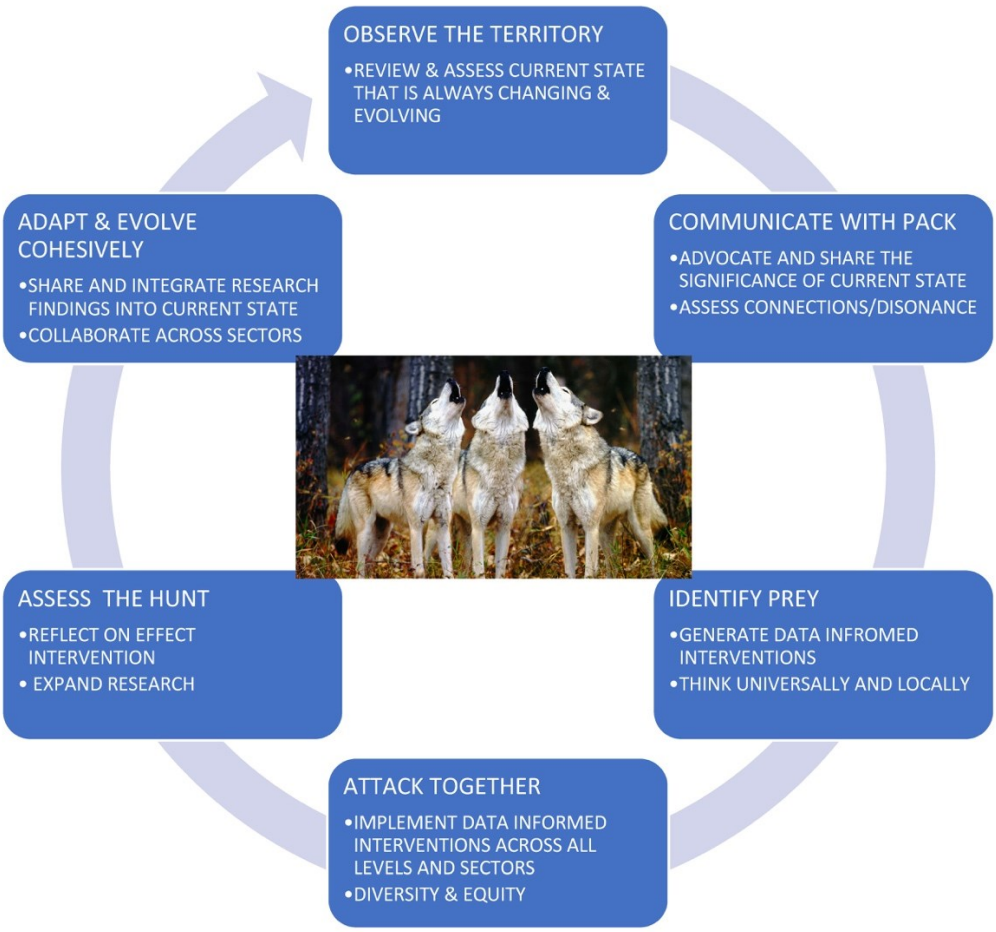
FIGURE 3
The Ethical Triangle (Svara, 2011)



CREATING & IMPLEMENTING A NATIONAL CYBER ETHICS EDUCATION MODEL

In response to the current limitations in cyber ethics education in the U.S. and the increasing pace and scale of cyber threats and attacks, a national cyber ethics education 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.

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



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 cyber ethics 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 U.S., 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.

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 Pray," 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 pro-actively 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. pro-active. Wolves who cannot identify the prey accurately and quickly may unexpectedly find themselves becoming the prey.

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 U.S. 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.

THE LEADING ROLE HIGHER EDUCATION & MILITARY CAN PLAY IN CREATING CYBER ETHICS EDUCATION MODEL

An interdisciplinary and inter-industry approach to cyber ethics education is required as the impact of cyber-threats and cyber-attacks is broad 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.

A CALL TO ACTION & RECOMMENDATION

In 2020, 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 bestowed a grim disguise. 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 though the development of increased education, research, and theory-building on cyber and data ethics. The U.S. is underprepared to ethically handle the pace and scale of our data and cyber use. Now is the time to heave Ian Malcolm's warning to investigate, study, and train ourselves to be more critical and ethical cyber users before we experience an unintended consequence or cyber-attack that leaves us incapable of rebooting.

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. (2000a). *Weaving the Web: The Orginial Design and Ultimate Destiny of the World Wide Web*. Harper Business.

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

Beuran, R., Tang, D., Pham, C., Chinen, K. ichi, Tan, Y., & Shinoda, Y. (2018). Integrated framework for hands-on cybersecurity training: CyTrONE. *Computers and Security*, *78*, 43–59. https://doi.org/10.1016/j.cose.2018.06.001

Beveridge, R. (2019). Effectiveness of Increasing Realism Into Cybersecurity Training. *International Journal of Cyber Research and Education*, *2*(1), 40–54. https://doi.org/10.4018/ijcre.2020010104

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*.

Chibbaro, J. S. (2007). School Counselors and the Cyberbully: Interventions and Implications. *Professional School Counseling*, *11*(1), 2156759X0701100. https://doi.org/10.1177/2156759x0701100109

Code.org. (2 C.E.). *Support K-12 Computer Science Education in Pennsylvania*.

Code.org. (2017). Should Computer Science Be A Mandatory Class In U. S. High Schools? *Quora*, 10–11.

Collaborate Ultra—File and Recording Storage FAQ. (2020, July 2). https://blackboard.secure.force.com/publickbarticleview?id=kA770000000CbqL

College Board. (2020). *AP Computer Science A Course at a Glance.* https://apcentral.collegeboard.org/pdf/ap-computer-science-a-course-a-glance.pdf?course=ap-computer-science-a

Conklin, W. A., Cline, R. E., & Roosa, T. (2014). Re-engineering cybersecurity education in the US: An analysis of the critical factors. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2006–2014. https://doi.org/10.1109/HICSS.2014.254

Corrin, A. (2011). Basic training enters unfamiliar territory in cyberspace. *Defense Systems.* https://defensesystems.com/articles/2011/11/28/feat-military-cyber-training.aspx

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

CSTA K–12 Computer Science Standards—Revised 2017, 1 (2017).

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

Dameff, C. J., Selzer, J. A., Fisher, J., Killeen, J. P., & Tully, J. L. (2019). Clinical Cybersecurity Training Through Novel High-Fidelity Simulations. *Journal of Emergency Medicine*, *56*(2), 233–238. https://doi.org/10.1016/j.jemermed.2018.10.029

Dawson, M. (2020). National Cybersecurity Education: Bridging Defense to offense. *Land Forces Academy Review*, *1*(97), 8–14. https://doi.org/10.2478/raft-2020-000

Education, C. S. (2019). *State of Computer Science Education Equity and Diversity*.

Goldstein, M. (2003). Congress and the courts battle over the first amendment: Can the law really protect children from pornography on the Internet? *The John Marshall Journal of Computer & Information Law*, *21*(2), 141–205.

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.

Gupta, D., Bajramovic, E., Hoppe, H., & Ciriello, A. (2018). The need for integrated cybersecurity and safety training. *Journal of Nuclear Engineering and Radiation Science*, *4*(4), 1–7. https://doi.org/10.1115/1.4040372

Hack Pennsylvania. (2020). About. https://hackpenn.com

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4), 249–257. https://doi.org/10.1080/10919392.2019.1611528

Higgins, S. (2014). Critical thinking for 21st-century education: A cyber-tooth curriculum? *Prospects*, *44*(4), 559–574. https://doi.org/10.1007/s11125-014-9323-0

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/

Jooinn. (2020). Pack of wolves. https://jooinn.com/img/startdownload

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.

Kirikkaleli, D., Abderrahmane, S., Candemir, M., & Ertugrul, H. M. (2018). Panel cointegration: Long-run relationship between Internet , electricity consumption and economic growth. Evidence from oecd countries. *Investigación Económica*, *LXXVII,*(303), 161–176.

Ku, R. S. R. (2002). The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology. *The University of Chicago Law Review*, *69*(1), 263–324.

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2019). The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-019-09977-z

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

Lee, P. (2016). Expanding the schoolhouse gate: public schools and the regulation of cyberbullying. *Utah Law Review*, *2016*(5), 831–.

Levy, S. (2010). *Hackers: Heroes of the Computer Revolution*. O'Reilly.

Lewandowski, J. (2002). Using Moral Development Theory To Teach K-12 Cyber Ethics. In N. D. D. Willis, J. Price (Ed.), *Proceedings of SITE 2002 Society for Information Technology & Teacher Education International Conference* (pp. 864–866). Association for the Advancement of Computing in Education.

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

Major League Hacking. (2020). *A high school's administrators guide to hacking*. https://mlh.io/high-school-administrator-hackathon-guide

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.

Middleton, B. (2017). *A History of Cyber Security Attacks 1980 to Present*. CRC Press.

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

NICE. (2020). Strategic Plan. https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan

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

OECD. (2019). Impact of Technology use on children: Exploring literature on the brain, cognition, and well-being. http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=EDU/WKP%282019%293&docLanguage=En

Oslejsek, R., Rusnak, V., Burska, K., Svabensky, V., Vykopal, J., & Cegan, J. (2020). Conceptual Model of Visual Analytics for Hands-on Cybersecurity Training. *IEEE 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.

Pruitt-Mentle, D., & Pusey, P. (2010). State of K12 Cyberethics, Safety and Security Curriculum in U. S: 2010. *Educator Opinion*. 18.

Pusey, P., & Sadera, W. A. (2011). Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference. *Journal of Digital Learning in Teacher Education*, *28*(2), 82–85. https://doi.org/10.1080/21532974.2011.10784684

Racheva, V. (2020). *What is virtual learning?* VEDAMO. https://www.vedamo.com/knowledge/what-is-virtual-learning/

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

Rodideal, A. (2018). Emerging Needs for Minimizing Negative Effects of Technology Overuse among Children. *Moldavian Journal for Education and Social Psychology*, *2*(1), 1–16. https://doi.org/10.18662/mjesp/01

Rotman, D. (2020, February 24). We're not prepared for the end of Moore's Law. *MIT Technology Review*, *123*. https://www.technologyreview.com/2020/02/24/905789/were-not-prepared-for-the-end-of-moores-law/

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. J. M. (2019). An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness Training Model (CATRAM). A case study in Canada. *Journal of Cases on Information Technology*, *21*(3), 26–39. https://doi.org/10.4018/JCIT.2019070102

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*. https://doi.org/10.1017/CBO9781107415324.004

Sobiesk, E., Blair, J., Conti, G., Lanham, M., & Taylor, H. (2015). *Cyber Education: A Multi-Level, Multi-Discipline Approach*. 43–47.

Spidalieri, F. and McArdle, J. (2016). Transforming the next generation of military leaders into cyber-strategic leaders: The role of cybersecurity education in US service academies. *Cyber Defense Review 1*, 1.

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

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

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

Taylor, J. (2012, Dec. 4). How technology is changing the way children think and focus. Psychology Today. https://www.psychologytoday.com/us/blog/the-power-prime/201212/how-technology-is-changing-the-way-children-think-and-focus

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. *National Assoication of State Boards of Education*, *23*(17).

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

Tucker, A. (2003). *A Model Curriculum for K-12 Computer Science*.

Ueno, T., & Maruyama, Y. (2011). The Significance of Network Ethics Education in Japanese Universities. *International Journal of Cyber Ethics in Education*, *1* (3), 50–58. https://doi.org/10.4018/ijcee.2011070105

University of Pittsburgh. (2020). *2020 Air Force Association Cyber Camp*. https://www.cyber.pitt.edu/2020-air-force-association-cybercamp

U.S. Cyber Command. (2020). *Mission.* https://www.cybercom.mil/About/Mission-and-Vision/

U.S. Cybersecurity & Infrastructure Security Agency. (n.d.). *What is Cyber Security?* 2020. https://www.us-cert.gov/ncas/tips/ST04-001

Vogels, E. A., & Anderson, M. (2019). *American and Digital Knowledge* (Issue October).

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.

Woodrow, M. (2014). *Cyber Security 2.0 and the History of the Internet* . Lulu Wnrwepeiawa Incorporated.

World Wide Web Foundation. (2020). *History of the Web*. World Wide Web Foundation. https://webfoundation.org/about/vision/history-of-the-web/

Woszczynski, A. B., & Green, A. (2017). Learning Outcomes for Cyber Defense Competitions. *Journal of Information Systems Education*, *28*(1), 21–42.

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

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

Yang, S. C. (2019). A curriculum model for cybersecurity master's program: A survey of AACSB-accredited business schools in the United States. *Journal of Education for Business*, *94*(8), 520–530. https://doi.org/10.1080/08832323.2019.1590296