# The B-School Knowledge Sharing Journey: How to Inform and Connect Cyber Ethics Education with the K-12 Pipeline

Jennifer Petrie-Wyman
University of Pittsburgh,
jlpetrie@business.pitt.edu

Anthony Rodi
University of Pittsburgh
afrodi@katz.pitt.edu

Richard McConnell
U.S. Army Command and General Staff College
richard.a.mcconnell4.civ@mail.mil

Patty D'Ascenzo
University of Pittsburgh

## ABSTRACT

*The COVID-19 pandemic has disrupted our lives in many ways. One key area of disruption has been in K-12 learning. As the world was thrown into fully remote environments, students of all ages were forced into a cyber learning environment with little to no preparation, as these challenges were unlike any other in education. Both educators and students found out very quickly how unprepared this remote learning environment was from a cyber preparation perspective. Knowledge sharing across higher-education institutions, industry, and K-12 schools have been challenging because foundational structures for collaborative partnerships were frequently absent. . The purpose of this paper is to start to address some of the cyber challenges experienced by K-12 education in the United States through the presentation of a collaborative cyber ethics leadership framework and to address the gaps in training and sharing of best practices through a cyber ethics training intervention called the Cyber Ethics Education Accelerator. This paper describes the positive knowledge sharing journey that can happen across Business schools (B-Schools), industry, and the K-12 sector.*

***Key concepts:***

1. ***Introduction: Realizing the K-12 Cyber Ethics dilemma***
2. ***A Review of Cyber Ethics Education in the United States***
3. ***The Cyber Ethics Leadership Framework***
4. ***The Knowledge Sharing Journey***
    a. ***Forming a cross-sector cyber ethics partnerships***
    b. ***Forging a cyber ethics accelerator for K-12 teachers***
    c. ***Challenges and Limitations***
5. ***The Call to Action in K-12 Teacher Training and Next Steps***

## INTRODUCTION

This paper examines the process and creation of cyber ethics education collaborative partnership intended to strengthen knowledge sharing across Business-Schools, higher education institutions, industry, and K-12 schools. The intent of the project is to ultimately provide support for under-resourced K-12 schools in the region through a community-partnership model attentive to supporting equity, diversity, and inclusion and social responsibility. This paper interrogates the literature and the limited cyber ethics resources available in American K-12 school (particularly in low socio-economic school districts), proposes a cyber ethics leadership framework, describes the creation of the Cyber Ethics Education Accelerator, (CEAA), and discusses future directions of practice and research.

As the COVID-19 pandemic has advanced, extensive vulnerabilities and inequities in the cyber landscape have unfolded across the United States. Educators, industry professionals, parents, and children all confronted cyber challenges. From the living room to the classroom, to the boardroom, we have all faced a new cyber reality that was complex and ever-changing. As a nation, we were at times prepared and comforted by our cyber capabilities as Zoom rooms and Google classrooms opened instantaneously in

April 2020. At the same time, this cyber capacity was inequitable, and the exponential expansion created heighted risks to users and systems. We confronted Google Classroom crashes, Zoom-bots, TikTok vulnerabilities, spotty connections, a minefield of fake news, toxic algorithms, and an escalation of cyber-attacks from nation-state actors. Many individuals forced into the remote environment used their own mobile devices and home networks, in place of company or school issued technology. Challenges experienced have been crowded home environments consisting of multiple people working from home causing restricted bandwidth, to unsecured devices causing multiple security vulnerabilities, to lack of access to high-speed internet particularly in low socio-economic and rural school districts (COVID 19: Cyber and the remote workforce, n.d.).

Cyber inequities and risks were particularly abundant throughout the K-12 educational system. In their paper, Garcia, et al, discusses the issue of "Learned Helplessness" as a result of remote learning and students required to use technology to replace the in-person learning environment and experiencing repeat failures of technology. This issue and impact on student learning has been caused by the sudden move to a fully remote learning environment without the proper preparation for engagement with new and unfamiliar technologies and the isolation experienced in a fully online environment (Garcia, et al, 2021). This sudden move to a fully online learning environment in K-12, has caused additional issues involving cyber vulnerabilities and cyber awareness. While higher educational institutions and businesses encountered cyber ethical challenges throughout the COVID-19 pandemic, the resource and training gap in K-12 schools was far greater leaving our K-12 system among the most vulnerable and resource deficient. This paper aims to start to address some of the cyber challenges confronting K-12 education through the presentation of a collaborative cyber ethics leadership framework and a cyber ethics training intervention called the Cyber Ethics Education Accelerator. The mission of the Cyber Ethics Education accelerator is to strengthen cyber ethics training and resources for K-12 schools, with an initial emphasis on low socio-economic and rural schools in Southwestern Pennsylvania. This paper describes the positive knowledge sharing journey that can happen across Business schools (B-Schools), industry, and the K-12 sector.

Gaps in training and knowledge-sharing across sectors left classroom teachers and school systems with a steep learning curving to rapidly remedy the challenges of virtual and hybrid learning. Amid learning new platforms, adapting curriculums, and communicating with students in an ever-changing hybrid context, addressing cyber risks and cyber ethics in K-12 schools often remained on the sidelines amongst the spiraling COVID-19 global pandemic. The impetus to adapt and use technology rapidly often came at the expense of critical conversations about our expanding cyber coverage in schools. In navigating pathways to confront and address the cyber dilemmas in K-12, the authors identified a need to advance cyber ethics collaborations including developing K -12 research frameworks and providing supportive and practical cyber ethics trainings and partnerships. The author's ABSEL paper in 2021 and publication in the *International Journal of Ethical Leadership* served as a theoretical research framework to advance cyber ethics educational and leadership dialogs. [1, 2] This paper, for ABSEL 2022, now suggests a practical cyber ethics knowledge sharing intervention to help support the development of cyber ethics training in K-12 schools.

Critical issues emerged from our ABSEL 2021 paper concerning our nation's cyber ethics education that we have integrated into our Cyber Ethics Education Accelerator intervention:

1. Lack of cohesion and coordination for cyber awareness
2. Glaring disparities and inequities across race, gender, and socioeconomics
3. No national cyber ethics education strategy
4. Very limited cyber ethics skill training across K-12 teachers and leaders
5. Lack of formal computer science and cyber-security training
6. Limited awareness of technology risk and safety in the classroom and remote environments

In this paper we will (1) review the cyber ethics education literature, (2) examine a cyber ethics leadership framework relevant to enabling cyber-ethics knowledge sharing across sectors, and (3) describe the knowledge sharing journey that occurred in our Cyber Ethics Education Accelerator. We will end with a (4) call to action in K-12 cyber ethics teacher training and next steps in the future of cyber ethics education.

## 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) .

[1] Petrie-Wyman, J., Rodi, A., & McConnell, R. (2021, March). Why Should I Behave? Addressing Unethical Cyber Behavior through Education. In *Developments in Business Simulation and Experiential Learning: Proceedings of the Annual ABSEL conference* (Vol. 48).

[2] Petrie-Wyman, J., Rodi, A., & McConnell, R. A. (2021). Where is the Justice? What We Don't Know about Cyber Ethics. *The International Journal of Ethical Leadership*, *8*(1), 94-115.

**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. Cyber ethics 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.

## A REVIEW OF CYBER ETHICS EDUCATION IN THE U.S. K-12 SCHOOLS

The growing concern for cyber ethics has 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).

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 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, as Coden Et al cautions, "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).

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 and to develop cyber solutions that promote justice, equity, and democratic rights.

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*, 2016b; Martin et al., 2015).

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 of 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 U.S. 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 Black Lives Matter movement is 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.

The inequities and shortfalls of computer science courses in K-12 schools also reflect a cyber training gap for teachers. (K-12 computer science teachers are limited throughout the U.S., both in terms of numbers of certified teachers and in attrition (*K12 Computer Science Framework*, 2016b). Computer science teachers are challenging to both recruit and retain in teacher preparation programs. A benchmark survey of certification requirements across Pennsylvania, New York, Colorado, and California reveal limited to non-existent coverage of cyber ethics. While most teacher-preparation programs do require a course in technology and learning, the content of most of these courses focus on pedagogic use and classroom management. Few courses give adequate basic training on cyber security and cyber ethics. Additionally, few professional development opportunities for K-12 teachers exist to strengthen their cyber knowledge. The limited coverage of cyber ethics in teacher preparation program is especially concerning given the increasing cyber threats to individual users, schools, and organizations across the U.S. and globally.

Another area of concern in cyber ethics education is the increasing rates of virtual learning and meeting fatigue, better known as Zoom fatigue, and teacher burnout (Bailenson, 2021). While virtual learning has created adaptability in the classroom, the burden of virtual learning and creating classroom adaptations have largely fallen to teachers themselves. Teachers have experienced a double burden of virtual fatigue, encountering long hours of virtual teaching alongside serving as the teacher, mentor, and coach to students confronting virtual fatigue themselves. Virtual Fatigue, as discussed by Shockley, et al, seems to be magnified by the constant use of camera during a virtual meeting. The pressure caused by constantly feeling the need to always be shown in a positive way, and the constantly feeling of always being watched during the meeting. The meeting participants tend to hold a gaze much longer, exhibit greater focus on the speaker, with exaggerated non-verbal actions such as head nodding, leading to greater fatigue during a meeting. Considering that these meetings may take place one after the other during the day, these constant behaviors may lead to exhaustion and fatigue over time (Shockley, 2021). Pressley (2021) adds to this research in the article discussion around K-12 teacher burnout. COVID-19 has caused additional stress and anxiety around the expectations for teachers regarding newer teaching requirements, parent interactions, student engagement and administrative demands (Pressley, 2021). Alarmingly, rather than supporting teachers, social media has often treated teachers as a scapegoat of public retribution over frustrations over virtual education failures, pandemic policies, staffing-shortages, and systemic failures in our nation's lack of preparation for a global pandemic. In the age of social media and politically motivated press, we have often blamed teachers for the cyber dilemmas we face, when in reality the dilemma is systemic in proportion crossing sectors and spanning decades of narrow foresight on how to ready our nation for a cyber world.

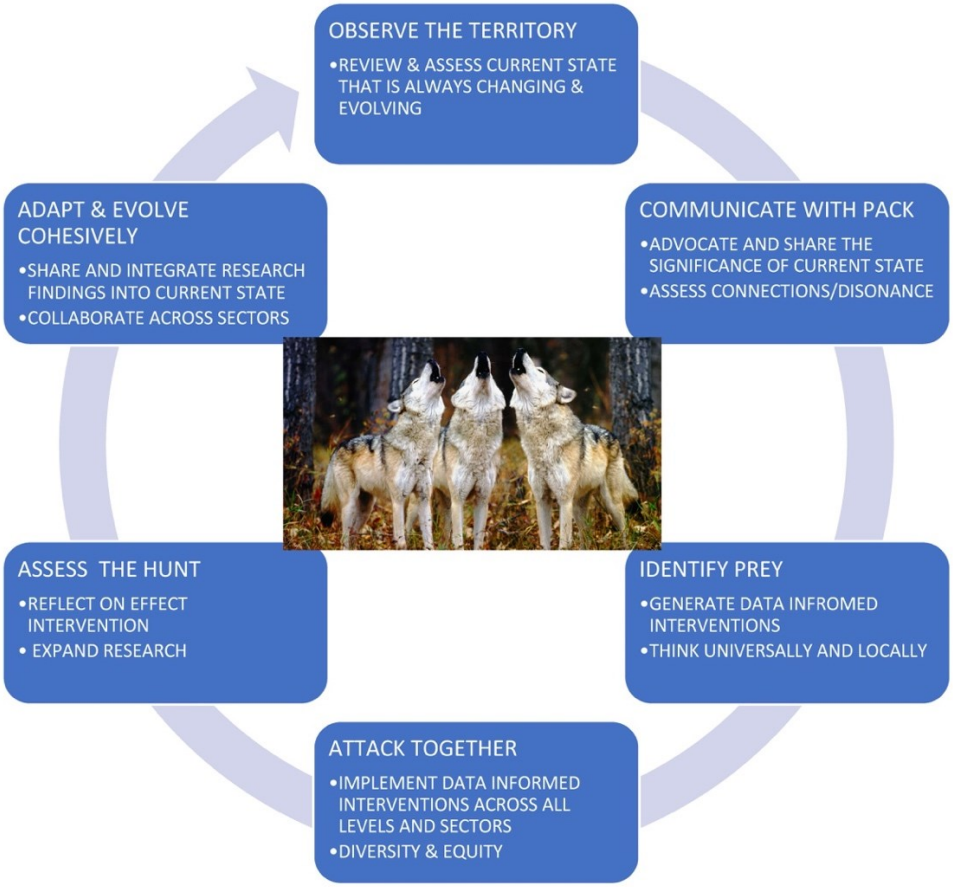
Since 2020, our nation's public school system has appeared bipolar. For some schools, the pandemic showcased schools appearing capable and innovative. For other schools, the pandemic propelled them to the brink of failure as they lacked the resources and coordination adapt to the challenges of the global pandemic. The global COVID-19 pandemic has created a need to deeply reconsider and reflect on the inequities and risks in our cyber schooling. For a more comprehensive review of cyber ethics education literature please see the author's 2021 publication in the *International Journal of Ethical Leadership*. [3]

## THE CYBER ETHICS LEADERSHIP FRAMEWORK

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 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 and was published in 2021.

**Figure 1. 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 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

[3] Petrie-Wyman, J., Rodi, A., & McConnell, R. A. (2021). Where is the Justice? What We Don't Know about Cyber Ethics. *The International Journal of Ethical Leadership*, *8*(1), 94-115.

currently available.

The Cyber Ethics Education Accelerator (CEEA) intervention described in this paper is attentive to steps 1-4 in the model and aims to develop steps 5-6 as the intervention is implemented. The intervention is rooted in step-1 of the model by utilizing a broad review of the current state of cyber ethics, "Observe the Territory," The CEEA is also attentive to the second step of this model, "Communicate with the Pack," as a cyber ethics education intervention is developed and shared across sectors and disciplines. The CEEA follows the third step of this model, "Identify the Prey," focusing on the specific needs of the sector and current state. The creation of the CEEA itself manifests as the fourth step in the model, "Attack Together," supporting 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.

The Wolftrap change model is appropriate for application in cyber ethics because of its organic nature of gaining understanding of an environment and reacting to it communally. In his paper *Why computers will never write good novels*, Angus Fletcher asserts that computers think algorithmically whereas people think narratively. Human communities are connected by and defined through their ability to think creatively using narrative (Fletcher, 2021). Therefore, since computers do not think like humans do, it is appropriate to apply a change model that epitomizes story/narrative thinking. The pack thanks organically and adapts to its environment. To address cyber ethics dilemmas, we should think less algorithmically and more narratively.

Fletcher, A. (2021). Why computers will never read (or write) literature. *Narrative*, *29*, 1–28.

## KNOWLEDGE SHARING JOURNEY OF THE CYBER ETHICS EDUCATION ACCELERATOR

Over the past year, the authors have been involved in creation of a collaborative program called the Cyber Ethics Education Accelerator (CEEA) focused on providing cyber ethics education training to local high school teachers in Western Pennsylvania. The central goal of the CEEA project was to provide cyber ethics training and resources to high school teachers to strengthen cyber ethics education in the curriculum and create a more knowledgeable workforce to reduce cyber-security risks in schools. The CEEA evolved out of discussions with the authors and cross-disciplinary group of faculties across the University of Pittsburgh to create broader opportunities to critical examine the role of cyber technologies inclusive of diversity and equity and community outreach. The Institute for Cyber Law, Policy, and Security also provided grant support to launch new cyber related programs and initiatives, which the authors were awarded in Winter 2020. Over the past year, faculty from the University of Pittsburgh's Katz Graduate School of Business and College of Business Administration, the School of Education, the U.S. Army Command and General Staff College, industry professionals, and educators across school districts in Western Pennsylvania have developed interdisciplinary dialogs regarding cyber ethics education and developed the first pilot teacher training for cyber ethics in the state of Pennsylvania. Working across the disciplines, the authors developed a mutually beneficial knowledge sharing journey across disciplines.

The knowledge sharing journey identified the need to expand the interdisciplinary focus of cyber ethics to support the development of a more diverse and ethical cyber workforce spanning across business, the public sector, and STEM industries. The project was also coordinated with potential policy implication such as creating certificate at the state level to develop synergy around cyber ethics across teaching subjects and administrators. The cyber ethics teacher training certificate can also be adapted applicable to professional development other disciplines, industry sectors, and institutions that face escalating cyber threats. For example, the U.S. Army includes professional development through Additional Skill Identifies (ASI) that could include attention to cyber ethics. The CEEA project centered on three core objectives:

1. Improve the pipeline of underserved students entering the cyber workforce by integrating cyber ethics into core subjects.
2. Expand the abilities of existing K-12 teachers in Western Pennsylvania to be more prepared, skilled, and agile in cyber ethics to support and amplify student interest and excellence in cyber education.
3. Share pilot training findings with the PA Department of Education and educator and industry professional nationally to strengthen cyber ethics education and leadership development

In building the CEEA, the authors coordinating with educators and industry professionals to develop training format, module content, and assessment and evaluations. The CEEA training happens in an online asynchronous format delivered through the Pitt Professional Teaching Platform, a virtual learning platform available for non-Pitt students. The Pitt Professional platform is part of a strategic initiative at the university to expand equity and access to Pitt education across the city of Pittsburgh and Western Pennsylvania region. The format of the CEEA consists of three core modules as well as a short introduction and concluding module. The module is intended to take participants 8 hours, and participants received an honorarium provided by the grant for their participation. The module training was guided by key learning outcomes:

1. Educators will develop a critical awareness of cyber technology by being an active user of technology vs. passive user of technology.
2. Educators will demonstrate an understanding of core concepts of cyber safety for schools including: data-security, data-privacy internet safety, hacking risks, cyber bullying, social media safety.
3. Educators will increase their cyber ethical awareness by learning essential cyber ethics frameworks.
4. Educators will learn the foundations of diversity, inclusion, and justice in the cyber education.
5. Educators will evaluate their current cyber ethics knowledge and perform a SWOT analysis of available school resources for cyber ethics.

6. Educators will create an introductory cyber ethics lesson plan specific to their grade-level and content area.
7. Educators will assess and articulate the value and consequences of emerging technology.

The module training aims to deliver the learning outcomes to participants. The outline for the 5 training modules is listed below with core learning objectives listed related to cyber-skill development and cyber ethics awareness. We also incorporated learning objective alignment to the Danielson Framework, an evaluation metrics for effective teaching

1. Introductory module
    a. The activities in this module will offer an introduction to the concepts of cyber security, cyber ethics, and cyber justice. In addition to introducing these concepts, the activities in this module will help you consider how they apply to your experience as an educator.
    b. Educators will be introduced to the training objectives, expectations, and general housekeeping issues, including submitting assignments, assignment expectations.
    c. Educators will initiate a KWL Chart (KWL to be re-evaluated at the end of the program). A KWL chart is a graphic organization tool to help participants reflect on the learning process from a constructivist perspective.. KWL stands for " What I know," "What I want to know," and "What I learned"
    d. Danielson Framework:
        - 1c Setting Instructional Outcomes

2. Cyber Ethics 101
    α. Educators will develop a critical awareness of cyber technology by being an active user of technology vs. passive user of technology.
    β. Educators will demonstrate an understanding of core concepts of cyber safety for schools including data-security, data-privacy internet safety, hacking risks, cyber bullying, social media safety.
    χ. Danielson Framework Teaching Domains:
        - 1c Setting Instructional Outcomes
        - 1d Demonstrating Knowledge of Resources
        - 2d Managing Student Behavior
        - 3a Communicating with Students
        - 4d Participating in a Professional Community
        - 4f Showing Professionalism

3. Introduction to Cyber Ethics in K-12
    a. Educators will evaluate their current cyber ethics knowledge and available school resources for cyber ethics. -- SWOT ANALYSIS
    b. Educators will increase their cyber ethical awareness by learning essential cyber ethics frameworks such as the ethical triangle
    c. Educators will examine their own ethical framework by examining what are their non-negotiables.
    d. Danielson Framework Teaching Domains:
        - 1d Demonstrating Knowledge of Resources
        - 2a Creating an Environment of Respect and Rapport
        - 2c Managing Classroom Procedures
        - 2d Managing Student Behavior
        - 4a Reflecting on Teaching
        - 4d Participating in a Professional Community
        - 4f Showing Professionalism

4. Cyber Justice K-12
    a. Educators will learn the foundations of diversity, inclusion, and justice in cyber education.
    b. Educators will assess and articulate the value and consequences of emerging technologies
    c. Danielson Framework
        - 1b Demonstrating Knowledge of Students
        - 1c Setting Instructional Outcomes
        - 2a Creating an Environment of Respect and Rapport
        - 2b Establishing a Culture for Learning
        - 3c Engaging Students in Learning
        - 3e Demonstrating Flexibility and Responsiveness
        - 4a Reflecting on Teaching

5. Concluding Module
    a. Educators will reflect on the recent learning opportunity and will consider their knowledge base before engaging in learning and evaluate their current knowledge base.
    b. Educator will share feedback on learning opportunity
        - Daniels Framework:
        - 4a Reflecting on Teaching

In addition to the learning objectives, each module adheres to a specific learning template that includes written introduction to module, video introduction to the module by faculty, learning activities, vocabulary to support the lesson, lesson assignments, and module summary. The assessment criteria are grounded in the Danielson Framework focusing on formative growth of educators across planning and preparation, instructional content, classroom environment, and professional responsibilities of educators. A sample of assignments given the training include: (1) self-reflective discussion boards on teaching practice, (2) reflective discussion boards on classroom and school environment, (3) reflective writing on integrating cyber ethics theory with education practice, (4) a cyber security 101 WebQuest, and (5) the creation of an integrated cyber ethics lesson plan.

The authors have provided a PDF that shows the overview Webpage of the introductory module and Module 1 in the appendix. Module 1, as shown in the Appendix, was created as an integrated knowledge transfer to include various disciplines such as Cyber Ethics, Education and Business. This multidisciplinary knowledge sharing is based on lessons learned during the COVID-19 experiences in both K-12 and higher Education environments. The module is designed as introduction for K-12 teachers to explore Cyber Ethics and to understand the importance of Cyber Awareness. The introductory module targets high school teachers, with activities aligned with the Danielson Framework and Cyber Ethics training, and discussions that are designed to connect and share thoughts and best practices with other educators. In addition, the module contains Cyber Ethics resources, articles, video's to provide additional Cyber awareness and reflection activities to reinforce learning.

The CEEA training and module objectives and activities will be reviewed in the pilot-phase of the project during the winter/ spring of 2022 and necessary changes will be implemented to the formal training during the summer of 2022. The formal training will be released to educators in Southwestern Pennsylvania in the summer/fall of 2022.

## A CALL TO ACTON FOR K-12 TEACHER TRAINING

Cyber-ethics education should be integrated into teacher-training programs to instruct teachers on the cyber-ethics dimensions for students and 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).

The pandemic has created the most virtually interconnected world due to the need to quickly adapt to a sudden remote environment. This accelerated adoption to new technologies has enabled organizations to adjust to social distancing to work and learn from home on a global scale. As a result of the quick adoption of technologies, the already under-prepared workforce lacked training and awareness of the consequences of the evolving cyber world. In addition, K-12 teachers were already unprepared for the cyber world and struggled to overcome challenges of being thrown into the remote environments.

As K-12 educators are transitioning back to classrooms, the challenges are not ending. With uncertainty still present, and the threat of returning to fully remote learning as a constant threat, teachers are still unprepared from a cyber awareness perspective. While they have grown accustomed to using new and different technologies to provide student engagement, the threat of cyber security vulnerabilities has not gone away. The need for Cyber Education Training is needed and will play an important role in better preparing our K-12 educators.

Future directions for the CEAA project include making the training available at no-cost to all teachers in Southwestern Pennsylvania. Additionally, the authors intend to disseminate and share findings across educators in Pennsylvania and nationally. The CEAA will also include training evaluations for participants aimed at continuous improvement and agility to the rapid pace of technology advances and cyber security threats.

Finally, K-12 educators must be creative and critical thinkers. Tremendous reserves of creativity had to be employed to come up with the adaptive solutions that took place during the pandemic. Although that rapid change created conditions that could lead to cyber ethical dilemmas, it also led to tremendous opportunities for improvements in pedagogy. Those opportunities should not be squandered. To face the challenges of an uncertain future, K-12 educators must improve their ability as creative thinkers with the capacity to imagine future states. In his book, *the premonition: a pandemic story*, Michael Lewis discusses how the pandemic was predicted by numerous public health officials who employed prediction, imagination, and forecasting (Lewis, 2021). The many lessons learned during the pandemic does constitute an incredible opportunity for improvements in education while also presenting possible threats in the area of cyber ethics. Therefore, K-12 educators need to be able to have the adaptive mindset to protect students and faculty while maximizing the opportunity to improve learning.

This paper contains numerous descriptions of knowledge sharing and collaboration between institutions such as the U.S.

Army command and General staff College and the University of Pittsburgh which yielded collaborative studies and publications. This collaboration was enabled by technology throughout which is a good thing. These collaborations are continuing into the future. The authors of this paper are continuing to work together to develop K-12 cyber education. Currently, there is a study to improve creative thinking instruction at the U.S. Army command and General staff College using narrative techniques proposed by Angus Fletcher at Ohio State University Project Narrative which represents an opportunity to improve creativity instruction (Fletcher, 2021). Similar techniques are currently being employed at University of Chicago Booth School of Management by Professor Greg Bunch. These collaborations enrich scholarship and practice and are all enabled by technology. The authors of this paper are arguing that although these are opportunities and are beneficial, with these opportunities comes potential threats as cyber bad actors seek to find ways to exploit opportunities and turn them into threats for people in the cyber domain. Educators within the K-12 discipline will need increased understanding of cyber ethics, creativity and imagination to understand where those opportunities can be turned into threats, and employee the Wolf trap change model to adjust to this new situation. The pandemic made this adaptation necessary. It is now time to understand how best to share knowledge while protecting individuals through cyber ethics.

**Figure 2. Call to Action/Future Research Topics**

## REFERENCES


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

Bailenson, J. N. (2021). Nonverbal overload: A theoretical argument for the causes of Zoom fatigue. *Technology, Mind, and Behavior*, *2*(1).

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

Deloitte. (n.d.). COVID-19: Cyber and the remote workforce How cyber vulnerabilities and operational efficiencies are reshaping the "next normal." https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-covid-19-cyber-and-the-remote-workforce.pdf

Education, C. S. (2019). *State of Computer Science Education Equity and Diversity*.Fletcher, A. (2021, May 12). *Angus fletcher project narrative*. https://projectnarrative.osu.edu/about/current-research/research-projects/angus-fletcher

Garcia, A., Powell, G., Arnold, D., Ibarra, L., Pietrucha, M., Thorson, M., Verhelle, A., Wade,N., and Webb, S. (2021). *Learned helplessness and mental health issues related to distance learning due to COVID-19.* In CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '21 Extended Abstracts), May 8–13, 2021, Yokohama, Japan. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3411763.3451526

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: 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.

Lewis, M. (2021). *The Premonition: A Pandemic Story*. W. W. Norton & Company.

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.

Nadler, R. (2020). Understanding "Zoom fatigue": Theorizing spatial dynamics as third skins in computer-mediated communication. *Computers and Composition*, *58*, 102613.

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.

Pressley, T. (2021). Factors Contributing to Teacher Burnout During COVID-19. *Educational Researcher*, 0013189X211004138.

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/

Shockley, K. M., Gabriel, A. S., Robertson, D., Rosen, C. C., Chawla, N., Ganster, M. L., & Ezerins, M. E. (2021). The fatiguing effects of camera use in virtual meetings: A within-person field experiment. *Journal of Applied Psychology*, *106*(8), 1137.

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.

Sokal, L., Trudel, L. E., & Babb, J. (2020). Canadian teachers' attitudes toward change, efficacy, and burnout during the COVID-19 pandemic. *International Journal of Educational Research Open*, *1*, 100016.

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

## APPENDIX.

# Breakout: Introductory Module

### Proposed Cyber Ethics Pilot Training for High School Teachers

**Introduction Module**

### Objective(s)

•Educators will be Introduce the training objectives, expectations, and general housekeeping issues, including submitting assignments, assignment expectations
•Educators will begin to make connections between the learning opportunity they are engaged upon and the Danielson Framework for teaching
•Educators will initiate a KWL Chart

### Activities

1. Watch welcome/course introduction video (1 minute)
2. Read directions for training. (2 minutes)
3. Read introduction on connecting Danielson Model and the PCAG Cyber Ethics training
4. Download the Danielson Framework Summary Chart (link) for use at the end of each learning module.
5. Read excerpt from *Where's the Justice: What we Don't Know about Cyber Ethics?*
6. Watch Path to Pedagogical Change (5 minutes)

7. Complete Pre-Course Survey
8. Begin the KWL Chart
9/ Access/download resources

### Assessment

No assessment will be made for this module. Instead, participants will be required to partake in the pre-course survey.

### Resource(s)

- PA State Standards for Computer and Information Technology
- Vocabulary terms/definitions list **break-out into each section
- Danielson Framework
- PA Framework for Evaluation: Classroom Teacher

# Breakout: Module1

### Proposed Cyber Ethics Pilot Training for High School Teachers

### Module 1: Cyber Security 101 & Digital Citizenship

### Objective(s)

- Educators will develop a critical awareness of cyber technology by being an active user of technology vs. passive user of technology.
- Educators will demonstrate an understanding of core concepts of cyber safety for schools including data-security, data-privacy internet safety, hacking risks, cyber bullying, social media safety.

### Activities

1. Watch module introduction video (2 minutes)
2. Read article: What it Takes to Move from a Passive to an Active Tech User (5 minutes)
3. Watch video: Cyber Ethics (13:57 minutes)
4. Modified Cyber Ethics discussion question – expectation short written summary of teacher reflections
5. Watch video: Six Degrees of Information (7:26 minutes)
6. Discussion post: possibly what does digital citizenship mean to you? How can you promote good digital citizenship in your classroom? (15 minutes)
7. Update KWL chart (10 minutes)

### Assessment

- Knowledge check - possibly two questions reflecting on above materials. (10 minutes)
- Discussion Board-Post

### Resource(s)

- Cyber Security 101 Vocabulary List
- Cyber Bullying Documentary