Jl. of Technology and Teacher Education (2022) **30**(2), 275–287

Promoting Interdisciplinary Integration of Cybersecurity Knowledge, Skills and Career Awareness in Preservice Teacher Education

KARA DAWSON
University of Florida, USA
dawson@coe.ufl.edu

PAVLO ANTONENKO
University of Florida, USA
p.antonenko@coe.ufl.edu

ZHEN XU
University of Florida, USA
xuzhen0508@ufl.edu

CHRISTINE WUSYLKO
University of Florida, USA
c.wusylko@ufl.edu

DO HYONG KOH
University of Florida, USA
dohyong.koh@coe.ufl.edu

K-12 teachers and students are vulnerable to cybersecurity attacks and mostly ill-prepared to deal with them. The COVID-19 pandemic has only increased these risks because of the reliance on digital technology in education and increased free time young children and adolescents spend online. Simultaneously, the U.S. is facing an extreme shortage of cybersecurity professionals. Given the rise of cyberattacks and the need for cybersecurity professionals, a concerted effort to prepare preservice teachers to integrate cybersecurity education across the K-12 curriculum is needed. In our vision for

2025, all preservice teachers across the country are prepared to integrate age-appropriate cybersecurity concepts, skills and career awareness in the curriculum regardless of their content area or grade level specialization. We propose a repository of stand-alone activities and full curricula developed through collaboration among K-12 educators, teacher educators, and cybersecurity experts that could be adopted across teacher education programs. We use the elementary grades as a context for providing examples of some activities that might be included in the repository. We also provide recommendations for developing such a repository and for individual teacher educators who want integrate cybersecurity education in preservice teacher education right now.

INTRODUCTION

The COVID-19 pandemic has resulted in an increased reliance on digital technology in education, which led to unprecedented cyberattacks on educational institutions including colleges and universities (Whitford, 2022) and K-12 schools (Attanasio, 2022; Levin, 2022). In addition, the pandemic has increased the free time young children and adolescents spend online which has, in turn, increased cyberattacks (FBI, 2020; Jargon, 2020), including attacks on young children involving financial (Chalk, 2022) and social emotional (Perez, 2018) consequences.

The aforementioned attacks coupled with other cybercrimes would constitute the world's third-largest economy after the US and China and its costs are expected to reach $10.5 trillion annually by 2025, up from $3 trillion in 2015 (Morgan, 2020). These annual costs are exponentially larger than the damage inflicted from natural disasters in a year, and hackers' profits today account for more than the global trade of all illegal drugs combined.

Despite the prevalence of and consequences from cyberattacks, the National Initiative for Cybersecurity Education reports that the US has almost 464,420 unfilled cybersecurity positions (CyberSeek, 2021). Some point to an unbalanced professional demographic as directly attributing to the lack of US cybersecurity professionals (Shumba, 2014) with the U.S. Bureau of Labor Statistics (2021) reporting that only 11% of information and security analysts are women and only 12% are African American.

During the height of the pandemic, President Biden elevated attention to the nation's cybersecurity challenges by issuing an Executive Order (U.S. Government, 2021) stating that "incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life." To address the cybersecurity challenges in K-12 education, the US Department of Education and its Readiness and Emergency Management for School Technical Assistance Center (REMS) have released a number of factsheets, guidelines and other publications for K-12 education leaders and IT professionals such as "Cybersecurity Considerations for K-12 Schools and School Districts" (REMS, 2017).

We contend that teacher education programs need something similar to an executive order to support teachers and students in addressing cybersecurity at school and in the home and in promoting cybersecurity career awareness. The little research related to cybersecurity and K-12 teachers and students is alarming. One of the largest studies involving 2703 students and teachers from 17 states classified K-12 teachers and students as high-risk for cybersecurity attacks based on their performances on cybersecurity judgement tasks with students performing worse than teachers and younger students performing worst of all (Yan et al., 2021). This study also found that cybersecurity judgement can be improved with education, support, and practice (Yan et al., 2021). Another study with 329 children aged 8 to 11, showed that participants generally felt safe online and thought highly of their ability to protect themselves. Yet, they were unable to articulate dangers they might face online or strategies they might take to protect themselves. These results were exacerbated for boys and younger children (Macaulay et al., 2021).

Some efforts to combat the lack of cybersecurity knowledge and shortage of cybersecurity professionals are underway at the K-12 level. In many cases these efforts begin in secondary school. For example, curricula for high school teachers have been developed (Javidi & Sheybani, 2018) and summer camps for high schoolers have been offered (Chen & Mosely, 2019). GenCyber is one such summer program that provides cybersecurity experiences for students and teachers at the secondary level and paves new pathways for broadening representation in cybersecurity related degree programs and careers (GenCyber, n.d.). In addition, New York has Computer Science and Digital Fluency Learning Standards that include a section on Cybersecurity (New York Department of Education, 2020) and K-12 teachers are a secondary audience for Association for Computer Machinery (ACM) curriculum guidelines for postsecondary degree programs (ACM,

2017). Fewer attempts have been made to bring cybersecurity knowledge and career awareness to elementary students but recent results suggest elementary students are capable of learning cybersecurity concepts and understanding about cybersecurity careers (Antonenko et al., 2022; Dawson & Antonenko, 2021).

While cybersecurity education in K-12 schools is sporadic, efforts in preservice teacher education are almost non-existent even though scholars identified preservice teachers' lack of cybersecurity knowledge over a decade ago (Pusey & Sadera, 2011). Cybersecurity is on the periphery of ISTE's Citizen Standard for Educators with the phrase "model and promote management of personal data and digital identity and protect student data privacy" but otherwise absent from preservice teacher education standards and curricula. Given the rise of cyberattacks and the need for cybersecurity professionals, a concerted effort to prepare preservice teachers to integrate cybersecurity education across the K-12 curriculum is needed.

VISION

In our vision for 2025, all preservice teachers across the country are prepared to integrate age-appropriate cybersecurity concepts, skills, and career awareness in the curriculum regardless of their content area or grade level specialization. Consequently, teacher educators need the knowledge and resources to prepare their students to be cyberaware and cybersmart citizens of the 21st century society. One could note that teacher education programs are already packed with content, standards, and accreditation requirements but we argue that these programs cannot afford to ignore such a salient and societally important area.

Cybersecurity can be simply defined as protecting information online and cryptology, or the science of making and breaking secret codes, is considered the backbone of cybersecurity (Paar & Penzl, 2010). Within these simple definitions are innumerable opportunities for teacher educators to bring cybersecurity education to preservice teachers who will then bring this content into K-12 schools. We envision a repository of activities and resources developed in collaboration with teacher educators, K-12 teachers and cybersecurity experts and aligned with relevant guidelines for teaching cybersecurity such as the NICE Framework for Cybersecurity Workforce Development (National Initiative for Cybersecurity Careers and Study, n.d.). After reviewing standards such as the NICE framework, separate standards for teachers related to cybersecurity education may need to be developed.

The repository would take advantage of existing resources (e.g., Common Sense Media) and also include new resources. In addition, we envision a mix of stand-alone activities and full curricula that could be adopted across teacher education programs, similar to how activities and entire curricula are now integrated to support Computer Science education in K-12 classrooms. We also envision a process by which teacher educators are provided support and guidance to both develop the relevant content knowledge and plan to integrate cybersecurity education; possibly through graduate certificates or micro credentialing (Burrows et al., 2021).

It may be helpful to think about specifically connecting cybersecurity to content areas and grade levels and to break cybersecurity teacher education into two areas: (1) skills and knowledge, and (2) career awareness. Although younger students have been shown to be vulnerable in cyberspace (Macaulay et al., 2021; Yan et al., 2021), few resources are available for the elementary grades. Young children can successfully learn about cybersecurity (Antonenko et al., 2022; Dawson & Antonenko, 2021) and we provide a few examples of the resources that might be available in the repository for elementary teacher educators.

Engaging students in making and breaking secret codes (i.e., cryptology) is a high interest, interdisciplinary way to introduce elementary students to cybersecurity (Antonenko et al., 2022). Teacher educators in an elementary social studies methods course could introduce cryptology when preparing preservice teachers to teach about World War II through discussion of the Navajo Codetalkers and WAVES (Women Accepted for Voluntarily Emergency Service). The Navajo Codetalkers were Native American people employed by the military during the war to use their oral language as a means of secret communication that was never deciphered during the war. WAVES was a little-known women's branch of the U.S. Naval Reserve where women were responsible for encoding and decoding messages intercepted during the war. Social studies educators could also discuss the importance of codes and symbols across different cultural contexts and how codes relate to modern cybersecurity. For example, one activity we developed for elementary students involves decoding the symbol for wisdom across Adinkra, Navajo and Ancient Chinese cultures (see Figure 1).

Figure 1. Symbols for Wisdom Across Cultures.

Teacher educators in an elementary language arts methods course could discuss techniques for deciphering secret messages and passwords such as frequency analysis which requires codebreakers to know the most commonly used letters in a particular language and how those letters most typically combine together to make words. Frequency analysis has connections to morphological awareness and can provide additional and stealthy opportunities for children to engage with the morphology of reading. In fact, preservice teachers could be guided to further promote stealth reading practices by introducing the two common types of ciphers. Substitution ciphers such as the Pigpen cipher used by the Freemasons substitute a symbol for each letter while transposition ciphers such as Scytale used by the Ancient Greeks rely on transposing letters around a war belt (or other appropriately-sized cylinder) to decipher messages. See Figure 2.

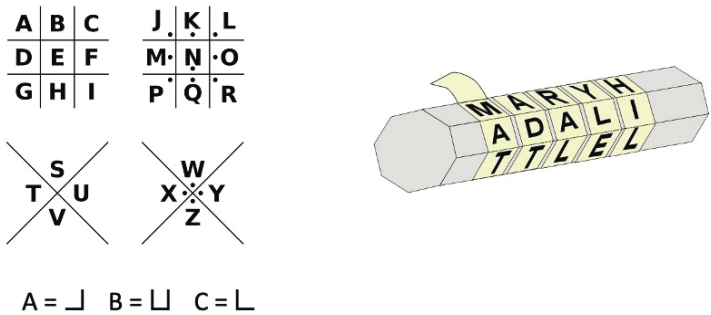


Figure 2. Pigpen Cipher and Scytale.

Elementary math educators can teach the concepts of positive and negative numbers and mathematic formulas using a Caesar Wheel which was developed by Julius Caesar to send secret messages to his generals in the field (Lunde, 2009; see Figure 3). Ciphers and codes are discussed very thoroughly in a mathematics focused curriculum aimed at middle schoolers in afterschool programs, called CryptoClubs (Beissinger & Pless, 2018).

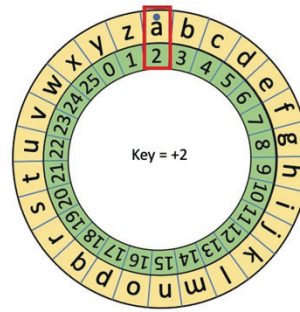


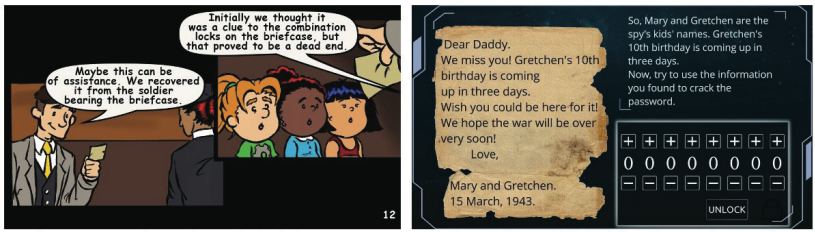
Figure 3. Caesar Wheel.

Elementary science educators could teach about acids and bases while students use invisible ink to encode and decode secret messages. Baking soda and water form the base of the invisible ink that allows students to create secret messages or symbols. Then, other students brush grape juice (the acid) over the secret messages to create a chemical reaction called neutralization that reveals the secret message (Xu, 2021).

Technology integration instructors could use ropes to help preservice teachers create a hands-on model of a working network and model how home networks could become vulnerable. Ropes represent edges in the network and notecards represent data packets. Students act as nodes, routers, or switches. First, a network is created by randomly distributing the rope to students. Then, students write a message on the notecard to identify a source and destination of the data packet. Sending the notecards down and along the ropes from the source to the destination allows for multiple opportunities to discuss the inter-workings of networks (e.g., routing, out-of-order delivery, packet loss, and man-in-the-middle attacks such as eavesdropping, packet manipulation, and packet dropping).

Finally, technology integration instructors could introduce concepts such as social engineering in which one's language and personal informa-

tion can be used to steal passwords. We use the example in Figure 4 in an elementary cybersecurity curriculum we developed. The curriculum is anchored in a comic book (Wusylko et al., 2022) and the main characters must use the information in a letter from the pocket of a spy to figure out how to get into his briefcase.



Social engineering activity begins in the comic book with Alan Turing showing the girls a note from the jacket pocket of a spy

A simulation with hints scaffolds the children to figure out the password for the spy's briefcase.

Figure 4. Social Engineering Activity.

The repository could also include online profiles of individuals with different strengths and interests and diverse representation in cybersecurity related careers. These may include language analyst, network penetration tester, network traffic analyst, crypto engineer, cybersecurity researcher and so on. For instance, the US National Security Agency is currently creating a collection of short and easy-to-understand videos discussing cybersecurity and cryptography careers (NSA, n.d.). Discussions of cybersecurity careers could be addressed in many K-12 subjects mentioned above. Additionally, teachers could integrate cybersecurity role model visits to increase students' awareness of the many career pathways available to them. Gender and race matched models are known to be particularly effective in terms of impacting student interest, identity, and self-efficacy for careers (Buck et al., 2008; Zirkel, 2002).

IMPLEMENTATION

Getting teacher education programs and teacher educators to buy into the interdisciplinary integration of cybersecurity education is a tall order, however, we have preliminary data to suggest preservice teachers would be receptive. We integrated a cybersecurity module into 4 sections of a Spring 2022 technology integration course for elementary majors and preliminary analysis suggests that preservice teachers went from thinking the topic was

somewhat irrelevant for elementary students to thinking it was an important (and fun) topic to integrate across the curriculum. Preservice teachers' self-efficacy about their ability to integrate cybersecurity in the elementary curriculum also improved. We also have data that suggests K-12 educators would be receptive to integrating cybersecurity skills and career awareness with educators saying this is a "game changer" especially for their female students. These educators worked with over 200 elementary school-age students – 73% girls – from diverse backgrounds and results suggest they enjoy learning about cybersecurity, rise to the challenge of encrypting and decrypting information using different ciphers and codes and transfer cybersecurity knowledge and skills to real-life (Xu et al., 2022).

A first step to reaching our vision for 2025 is to disseminate information about cybersecurity education in major teacher education outlets such as journals like the *Journal of Technology and Teacher Education (JTATE)*, *Contemporary Issues in Technology and Teacher Education* (CITE), the *Journal of Research on Technology in Education* (*JRTE*), the *Journal of Digital Learning and Teacher Education* (*JDLTE*), and at professional conferences.

Simultaneously, efforts must begin to compile a working group of teacher educators, K-12 teachers and cybersecurity experts interested in making the vision of a repository for preservice cybersecurity education a reality. The following action steps are recommended points for the working group:

1. Identify potential funding sources for the repository.
2. Identity national and state standards that align with cybersecurity education.
3. If necessary, develop standards specific to cybersecurity education for teachers.
4. Identify existing cybersecurity education resources.
5. Develop a mechanism by which curricula and resources can be submitted to the repository.
6. Develop a mechanism by which curricula and resources can be vetted.
7. Develop strategies to cross-walk the curricula and resources with standards, content areas, and grade levels.
8. Create opportunities for teacher educators to learn about the repository.
9. Create credentialing opportunities for individual teacher educators and for teacher education programs committed to integrating cybersecurity education.

This repository will take time and effort to develop. In the meantime, we encourage teacher educators to work within their own courses and programs to include cybersecurity in preservice teacher education. We offer the following suggestions to make these efforts most productive:

1. Demonstrate that cybersecurity careers are very diverse and welcome people with unique strengths in a variety of areas such as visuospatial reasoning, ability to identify patterns in text and numbers, knowledge of foreign languages and linguistics etc.
2. Align cybersecurity integration with workforce development frameworks such as the NICE framework (mentioned above).
3. Explicitly prepare preservice teachers to support self-efficacy and identity development for cybersecurity education and careers.
4. Relate cybersecurity integration to other approaches to broaden participation of women and underrepresented cultural minorities in STEM (i.e. NSF INCLUDES).
5. Highlight the relevance and importance of cybersecurity knowledge and skills across K-12 curricula by aligning cybersecurity integration with existing content area standards (NCSS, NCTE, NCTM, etc.).
6. Develop situational interest for preservice teacher (and eventually K-12 learners) by adopting situated and anchored instruction during cybersecurity integration.

The combination of disseminating cybersecurity information in teacher education journals, compiling a working group of teacher educators dedicated to creating cybersecurity repository, and including cybersecurity in preservice teacher education programs will achieve our vision. By 2025 we hope that all preservice teachers across the country are prepared to integrate age-appropriate cybersecurity concepts, skills and career awareness in the curriculum regardless of their content area or grade level specialization.

CONCLUSION

The lack of K-12 educational opportunities for cybersecurity in light of the increase in cybercrime during the COVID-19 pandemic coupled with the desperate need for increasing the number and diversity of cybersecurity professionals, present a challenge to teacher education we cannot afford to dismiss. While much work needs to be done between now and 2025, we have outlined a vision to help prepare teacher educators and their future students to meet this global challenge.

References

Antonenko, P., Xu, Z., Wusylko, C., Koh, D., & Dawson, K. (2022, June). *Engaging children in cryptology and cybersecurity learning and career awareness.* [Paper presentation]. American Society for Engineering Education, Minneapolis, MN.

Association for Computing Machinery. (2017). *Cybersecurity curricula: Curriculum guidelines for post-secondary degree programs in cybersecurity.* https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Attanasio, C. (2022, January 31). *Hackers prey on public schools, adding stress amid Covid pandemic*. PBS. https://www.pbs.org/newshour/education/hackers-prey-on-public-schools-adding-stress-amid-covid-pandemic

Beissinger, J., & Pless, V. (2018). *The Cryptoclub: Using mathematics to make and break secret codes*. CRC Press.

Buck, G., Plano Clark, V., Leslie-Pelecky, D., Cerda, P., & Lu, Y. (2008). Examining the cognitive processes used by adolescent girls and women scientists in identifying science role models: A feminist approach. *Science Education, 92*, 688–707.

Burrows, A. C., Borowczak, M., & Mugayitoglu, B. (2021). Computer Science beyond coding: Partnering to create teacher cybersecurity microcredentials. *Education Sciences*, *12*(1), 4–13.

Chalk, A. (2022, February 14). *A new report on Roblox reveals how hackers and scammers are continuing to rip off kids*. PC Gamer. https://www.pcgamer.com/a-new-report-on-roblox-reveals-how-hackers-and-scammers-are-continuing-to-rip-off-kids/

Chen, L., & Mosley, P. (2019) *Camp Cryptobot: Summer cybersecurity workshop for high school students at Pace University*. Department of Defense.

CyberSeek (2021). Cybersecurity supply/demand heat map. https://www.cyberseek.org/heatmap.html

Dawson, K., & Antonenko, P. (2021, December 14). *Comic book introduces kids to key concepts and careers in cybersecurity*. The Conversation. https://theconversation.com/comic-book-introduces-kids-to-key-concepts-and-careers-in-cybersecurity-171163.

FBI (2020). *2020 Internet crime report.* https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Gencyber. (n.d.). *Inspiring the next generation of cyber stars*. https://www.gencyber.com/about/

Jargon, J. (2020, September 8). *How kids' videogame accounts get hacked: Advice for parents*. *The* Wall Street Journal. https://www.wsj.com/articles/videogame-hackers-are-stealing-players-accounts-and-loot-during-pandemic-11599570006

Javidi, G., & Sheybani, E. (2018, October). *K-12 cybersecurity education, research, and outreach*. 2018 IEEE Frontiers in Education Conference (FIE) (pp. 1–5). IEEE.

Levin, D. A. (2021). *The state of K-12 cybersecurity: 2020 year in review*. EdTech Strategies/K-12 Cybersecurity Resource Center and the K12 Security Information Exchange. https://k12cybersecure.com/year-in-review/

Lunde, P. (2009). *The Book of codes: Understanding the world of hidden messages: An illustrated guide to signs, symbols, ciphers, and secret languages*. University of California Press.

Macaulay, P. J., Boulton, M. J., Betts, L. R., Boulton, L., Camerone, E., Down, J., & Kirkham, R. (2020). Subjective versus objective knowledge of online safety/dangers as predictors of children's perceived online safety and attitudes towards e-safety education in the United Kingdom. *Journal of Children and Media*, *14*(3), 376–395.

Morgan, S. (2020, November 13). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

National Initiative for Cybersecurity Careers and Studies (n.d.) *Workforce framework for cybersecurity*. https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework

New York State Education Department. (2020). *Computer science and digital fluency learning standards.* http://www.nysed.gov/common/nysed/files/programs/curriculum-instruction/computer-science-digital-fluency-standards-k-12.pdf

NSA. (n.d.). *NSA careers*. YouTube. https://www.youtube.com/user/WorkatNSA/videos

Paar, C., & Penzl, J. (2010). *Understanding cryptography.* Springer.

Perez, S. (2018, July 18). Roblox responds to the hack that allowed a child's avatar to be raped in its game. *TechCrunch*. https://techcrunch.com/2018/07/18/roblox-responds-to-the-hack-that-allowed-a-childs-avatar-to-be-raped-in-its-game

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.

REMS (2017). *Cyber safety considerations for K-12 schools and school districts*. https://www.schoolsafety.gov/resource/cyber-safety-considerations-k-12-schools-and-school-districts.

Shumba, R., Ferguson-Boucher, K., Sweedyk, E., Taylor, C., Franklin, G., Turner, C., & Hall, L. (2013, June 29). Cybersecurity, women and minorities: findings and recommendations from a preliminary investigation. *Proceedings of the ITiCSE Working Group Reports Conference on Innovation and Technology In Computer Science Education-Working Group Reports* (pp. 1–14). ITiCSE.

U.S. Bureau of Labor Statistics. (2021). *Labor force statistics for the current population surve*y. https://www.bls.gov/cps/cpsaat11.htm

U.S. Government. (2021). *Executive order on improving the nation's cybersecurity*. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Whitford, E. (2022). *Cyberattacks pose 'existential risk' to colleges-and sealed one small college's fate*. Forbes. https://www.forbes.com/sites/emmawhitford/2022/04/19/cyberattacks-pose-existential-risk-to-colleges-and-sealed-one-small-colleges-fate/?sh=25a671753c26

Wusylko, C., Xu, Z., Dawson, K., Antonenko, P., & Koh, D.H. (2022). *Using a comic book to engage students in a cryptology and cybersecurity curriculum.* [Paper presentation]. American Educational Research Association, San Diego, CA.

Xu, Z. (2021). *Making Adinkra Stamps*. YouTube. https://www.youtube.com/watch?v=yrNhWlBvCzs.

Xu, Z., Antonenko, P. Koh, D. H., Dawson, K., & Wusylko, C. (2022, April 21-25). *Scaffolding visuospatial cognition in a cryptology and cybersecurity curriculum for elementary students*. [Paper presentation]. American Educational Research Association, San Diego, CA.

Yan, Z., Xue, Y., & Lou, Y. (2021). Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. *Computers in Human Behavior*, *121*, 106791.

Zirkel, S. (2002). Is there a place for me? Role models and academic identity among white students and students of color. *Teachers College Record, 104*(2), 357–376.