THEME ARTICLE: **Curricular Foundations of Cybersecurity**.

Seeding Cybersecurity Workforce Pathways with Secondary Education

Jessica Ivy, Bellarmine University

Sarah B. Lee, Mississippi State University

Dana Franz, Mississippi State University

Joseph Crumpton, Mississippi State University

Integrating computational thinking and cybersecurity in K-12 classrooms is becoming increasingly essential to the development of a responsible and innovative workforce. To maintain competitiveness in a digital economy as a nation, the United States must broaden participation in computing and cybersecurity education and career pathways. This study examines professional development designed to foster the collaboration of from varying disciplines to study computing and cybersecurity concepts and plan for the integration of this content in their classrooms. The results of assessments at the beginning and conclusion of the experience provide insight into teachers' knowledge growth, their understanding of cyber principles, and the application of these principles in their classrooms.

Teachers and students are often unaware of the multi-disciplinary relevancy of computing and are unable to visualize the application of computational thinking to STEM pathways.[1] Cybersecurity is an integral part of these pathways, yet students often are unable to make the connection to their content area of focus. An understanding of safe, responsible online behavior is critical to the safety of all citizens, regardless of their role in society. Economic development is impacted by all of these issues, and economic growth is dependent on developing a workforce with computing and cybersecurity skills.

Advancing these skills in Mississippi (MS) is critical to the "growth, diversification, and competitiveness of the state's economy, which has traditionally lagged behind the nation and other Southeastern states in terms of employment growth, median income and tech sector employment."[2] With MS ranked last in the 2017 State New Economy Index published by the Information Technology & Innovation Foundation, the development of cybersecurity skills represents a new pathway to economic development and innovation and is critical to economic vitality in the state. [2] Out of 477,633 public school students in 2017-2018, 48.93% are female, 48% identify as African American, and 70% receive free or reduced meals in school.[7,8] One approach to reaching this diverse set of students is to engage public school teachers from a variety of disciplines in the study of cybersecurity and computer programming concepts and enable them to apply this knowledge in their classrooms.

Strengthening U.S. cybersecurity capabilities requires a comprehensive and coordinated effort to build the cybersecurity workforce[9], making this interdisciplinary approach both relevant and necessary. By developing a cybersecurity education pathway that standardizes transdisciplinary curricula and integrates with existing programs and taxonomies, a foundation for teacher accreditation will be realized.[9]

Mississippi, at present, does not have a licensure designation for computer science (CS) teachers; currently these teachers are licensed to teach other subjects and determined able to teach these courses through interest and loosely defined competence. However, this process is haphazard at best. To advance CS education in our K-12 schools, it is important to identify the best potential teachers. By meeting teachers in the comfort zone of their content areas, and engaging them with computing and cybersecurity concepts in the context of that comfort zone, teachers begin to build their self-identity with computing.[1] The Mississippi Department of Education does recognize the growing need for appropriately educated teachers as they have set a goal of having all K-12 students engaging in some type of CS learning by 2020. The Bulldog Bytes teacher development program at Mississippi State University (MSU) is laying the groundwork for all teachers to have the opportunity to engage with computer science, computer programming, and cybersecurity, based on a core belief that growing CS teachers from within the current teacher workforce is essential. The best computing teachers may come from the ranks of the music teacher, the history teacher, or the math teacher. With 37,000 teachers bringing these concepts and skills to the classroom, Mississippi has the opportunity to engage 400,000 students in pathways towards further education at the secondary education level and beyond, thus increasing the pool of cybersecurity education professionals.

Interdisciplinary approaches to cybersecurity education can be found in the literature. New England has a consortium that brings together different disciplines in order to make progress on cybersecurity issues, emphasizing that it takes expertise from many disciplines including national and homeland security, economics, law, psychology, sociology, and public policy in addition to mathematics, engineering, and computer science.[10] By providing teachers with different subject matter and the background to collaborate on teaching cybersecurity topics, a multi-level, multi-discipline approach to cyber education is created, with the goal of providing a level of cyber education appropriate for each person's role in society.[11] Offering electives in multiple departments, West Point demonstrates this interdisciplinary approach to cybersecurity education at the undergraduate level. Examples include a digital forensics course, an interdisciplinary cyber operations course that covers cyber law and cyber policy (co-taught by a computing faculty member and an International Relations faculty member), an Applied Algebra with Cryptology course taught by the Mathematical Sciences Department, and a Cyber Ethics course that is taught by the Department of English and Philosophy.[11]

BACKGROUND

The authors have developed a research-based professional development curriculum, Attract-Inspire-Mentor (AIM), for secondary education teachers to integrate computing and cybersecurity into their classrooms regardless of content area. The idea evolved from the Bulldog Bytes computing and cybersecurity K-12 student outreach program established at MSU in 2013. The program was initially funded through the National Center for Women & Information Technology's AspireIT program, and has received private funding throughout the years. The departments of Computer Science & Engineering (CSE) and Curriculum, Instruction and Special Education (CISE) at MSU began collaborating in 2014 to develop summer professional development workshops for in-service teachers across all disciplines to learn and bring computing, cybersecurity, and computational thinking into their classrooms. Since 2015, Bulldog Bytes has received funding from the National Science Foundation/National Security Agency GenCyber program to provide a platform for bringing cybersecurity and computer awareness and skills to students (elementary to high school) and K6-12 teachers in Mississippi. Facilitated through the Mississippi Computing and Cybersecurity Equitable Education Space housed at MSU, the AIM project-based curriculum introduces students and teachers to a diverse set of computing professionals and content, engaging them with:

- cybersecurity through hands-on independent and team modules,
- digital forensics with hands on case study projects,
- computer programming using robots, and
- team-based problem solving, design, and implementation.

Targeted participants for the summer teacher workshops include middle and high school teachers located in the state of Mississippi. Interested teachers are encouraged to apply regardless of the discipline they teach in order to promote the integration of cybersecurity concepts across curriculums. Priority admittance is given to teachers who fit one or more of the following criteria: (1) apply in teams of at least two, (2) have current or prior participating students in GenCyber student camps, and (3) demonstrate administrative support for implementing key ideas from the program. These workshops have informed the development of a credit course offering, Integrating Computing and Cybersecurity in the Classroom, for undergraduate and graduate pre-service teachers at MSU.

The Bulldog Bytes Workshops for Teachers have three primary goals: 1) increase cybersecurity knowledge and awareness in ways which align with teachers' respective content standards, 2) promote appropriate pedagogical practice which can be used to engage students in problem solving, collaborative and cooperative learning, and critical thinking skills vital to solving cyber challenges, and 3) plan lessons which integrate cybersecurity concepts in teachers' classrooms bridging cross-curricular content to cybersecurity topics.

Following the workshop, Bulldog Bytes Cyber Days are held to bring K-12 students from the community to the MSU campus to explore programming and cyber concepts. This provides an opportunity to further expand the reach beyond the classrooms immediately impacted with a follow-up mentoring component. Participating teachers can bring their students for this event also, with student limit dependent on available space.

IN-SERVICE TEACHER CURRICULUM

For one week, during content-focused lessons, teachers learn cybersecurity basics: security vulnerabilities, cybercrime, and how attention to safe online behavior is crucial to their personal safety. Teachers are taught computer programming using Sphero and Finch robots. All modules have one or more hands-on activity to facilitate a learner-centered environment. Industry speakers collectively introduce students to computing careers, with particular attention to cybersecurity career paths. Observations reveal that teacher participants network quickly with speakers and instructors during these experiences to gain resources for their classrooms.

Pedagogical-focused lessons involve topics which span across content areas such as grouping strategies, management techniques, questioning types, engaging students in productive struggle, and fostering classroom discourse. These sessions include professional readings, poster sessions, and small group discussions; which model appropriate teaching strategies. Resource texts, including a text on Digital Citizenship, offer base lessons which teachers adapt for their classroom use. These texts are explored during the workshops, and lesson development with feedback from other participants and the workshop facilitator is a daily occurrence.

Teacher assessments collect data before and after each workshop. Initial teacher applications assess their current levels of support and involvement in programming or cyber programs. At the conclusion of the week, a survey including open-ended reflection questions on cybersecurity concepts is administered. These assessments include the TPACK Developmental Survey which measures changes in teachers' Technological Pedagogical Content Knowledge (TPACK) for each discipline.[12] Teachers develop lessons that are classroom-ready when they leave the workshop. TPACK was selected as the lens for measuring teachers' growth in knowledge based on their experience because it captures data on teachers' knowledge of content, how to teach the content, and technology, as well as the knowledge. In other words, it is not enough to understand both content, technology, and teaching strategies. Rather, a teacher must understand how to use appropriate strategies and technology tools to enhance the teaching and learning of appropriate content. [13] TPACK is also useful because it considers themes including teaching, learning, assessment, equity, and access. The TPACK Developmental Survey, developed in 2011 and revised for this study, allowed teachers to consider first-person statements and indicate which statements best aligned with their beliefs and practices.[14]

Lessons developed are assessed using the EQUIP Quality Review Protocol[15], which is used to ensure key components of exploration, implementation, and discussion are present throughout lessons. Participants complete monthly logs post-workshop, demonstrating their integration of the lessons they implement. A final questionnaire is administered via a Google Docs form six months after workshop conclusion to assess self-reported longitudinal impact of the training on classroom instruction. These data components are used to assess the effectiveness of the program on teachers' practices as well as to guide decision making for future offerings.

On the final day of the workshop, teachers team with others in their discipline to refine their lessons, which integrate the concepts from the week and align with their curricular goals. Some teacher groups develop ideas throughout the week and formalize those into a well-organized unit by the final day. Other groups will craft one very detailed lesson or multi-day project that will function in more of a supplementary way to their curriculum. These are both acceptable, as the goal is for participating teachers to begin to integrate cybersecurity ideas during the first few weeks of their school year.

Learning Modules and Objectives

Daily learning modules integrate content for learning and teaching, with time for teachers to struggle productively as learners prior to integrating the new material into their curricular standards. The GenCyber Cybersecurity Principles[17] provide a basis for the new content knowledge. For each learning objective, activities to support a learning-centered classroom are provided in Table 1 with learning outcomes. The modules described are: Introduction to Cybersecurity, Digital Forensics and Cyber Crime, Introduction to Computer Programming, Engineering Design, Cryptography: Encryption and Decryption, and Career Exploration.

Table 1. Learning objectives and supporting activities.

Introduction to Cybersecurity
Learning Outcomes
Case Study showing how information posted causes a fictitious character problems through his/her life Students are prompted to offer input on how to prevent that scenario from happening Safe Passwords Activity
Activities
Demonstrate recognition of First Principles: data hiding, least privilege, layering, domain separation Be able to list risk of online activity and steps one can take to protect personal data and identity. Demonstrate understanding of basic client server architecture Demonstrate understanding of virtualization and storage media vulnerabilities Be able to compare and contrast at least two different types of operating systems Give an example of an ethical dilemma one might face in the cyber domain Demonstrate understanding of security countermeasures including firewalls and anti-malware software and techniques
Digital Forensics and Cyber Crime
Learning Outcomes
Demonstrate recognition of First Principles: data hiding, least privilege, layering, domain separation, abstraction, minimization data hiding, least privilege, layering, domain separation, abstraction, minimization Demonstrate understanding of write blocking Describe application of steganography and data obfuscation Describe how EXIF data is useful in forensic investigations Demonstrate an understanding of Alternate Data Stream and how it may be used
Activities
Capture the Flag Browsing History exercise using Autopsy Detecting Fake Photos Analyzing Email Analyzing Websites

Introduction to Computer Programming
Learning Outcomes
Demonstrate recognition of First Principles: minimization, conceptually simple, abstraction, modularity, resource encapsulation, process isolation Demonstrate, through individual and team project assignments, the ability to formulate project requirements and appropriate alternative solutions using Snap! (middle school) and Python (high school)
Activities
Individual tasks with Spheros Individual tasks with Finch robots Open Ended Student-drive Team Project
Introduction to Engineering Design
Learning Outcomes
Demonstrate recognition of First Principles: minimization, conceptually simple, abstraction, modularity, resource encapsulation, process isolation Demonstrate, through individual and team project assignments, the ability to formulate project requirements, identify design alternatives, and implement appropriate solutions
Activities
Design a robot (working in pairs) using Hummingbird Robot Kits
Cryptography: Encryption and Decryption
Learning Outcomes
Demonstrate recognition of First Principles: *data hiding* Describe the basic concepts of cryptography Demonstrate understanding of hash functions Describe data communication vulnerabilities
Activities
Encrypted Campus Scavenger Hunt Caesar Cypher encryption

Assessment Methodology

Data is collected, primarily through pre- and post- assessments. TPACK was selected as a key measure (through analysis of self-perceived levels), due to the program goal to increase teachers' knowledge for integrating technology in their content areas. Data is presented from the 2016 and 2017 workshops for 38 teacher participants. The program assessment consisted of three parts, TPACK Self-Reflection, TPACK Self-Assessment Survey, and Cyber Principles Assessment. Data and findings from these areas are provided below.

TPACK Self-Reflections

The TPACK Self-Reflection Survey included seven domain-specific items. The knowledge domains included: content knowledge (CK), pedagogical knowledge (PK), technological knowledge (TK), technological content knowledge (TCK), pedagogical content knowledge (PCK), technological pedagogical knowledge (TPK), and technological pedagogical content knowledge (TPACK). For each domain, participants rated their own levels of confidence, with descriptors ranging from "I am not sure what this means" to "I feel very confident in this area. I am a leader and a resource for other teachers." Each of the seven domain responses had four possible responses, so the maximum potential score for each item was 4, and the maximum score for this assessment was a 28. Data from the TPACK Self-Reflection are included in Table 2 and indicate the highest confidence growth in the TPACK Domain, followed by the Pedagogical Knowledge Domain, indicating that experiences with technology helped teachers build confidence in strategies used to teach. All rated as well or higher on the post- assessment than the pre- assessment, with an average growth on the 28-point index of 4.76.

Table 2. Summary of domain-level data from TPACK Self-Reflections.

Domain	Average at Pre	Average at Post	Change
CK	3.24	3.83	0.59
PK	2.86	3.59	0.72
TK	2.79	3.45	0.66
TCK	2.69	3.45	0.66
PCK	2.79	3.48	0.69
TPK	2.48	3.17	0.69
TPACK	2.45	3.21	0.76

TPACK Self-Assessment Survey

The TPACK Self-Assessment Survey included 11 categories, adapted from the themes and subthemes of the TPACK Development Model.[12] For each category, five levels of descriptors provided insight into the TPACK levels for participants. The five levels were recognizing, accepting, adapting, exploring, and advancing. Each level was correlated to a numerical value from one to five, and the sum of the criteria provided an indexed TPACK rating for each iteration of the TPACK Self-Assessment Survey. The average score for the pre-test was a 34 (out of 55), and the average score on the post-test was 42. This change represents a shift from 61% to 76%.

Cyber Principles Assessment

The Cyber Principles Assessment was administered pre- and post- program. This Assessment required participants to provide a definition for each of the ten cybersecurity principles and a description of connections to their classroom. The principles on the assessment were: domain separation, process isolation, resource encapsulation, least privilege, layering, abstraction, information hiding, modularity, simplicity of design, and minimization. It is notable that most left the pre-test blank, suggesting that the terms were completely foreign to them. The scoring of the Cyber Principles Assessment included rating each response from zero to three, for a total possible point value of 30 (15 for definition and 15 for connections). At the pre-assessment, the average values for definition and connections descriptors were 0.34 and 0.21, respectively. At post-assessment, the average values rose to 15.24 and 9.76, respectively. It is also notable that participants were much more confident and accurate in their definitions of the terms than the connections to their classrooms.

Implications and Conclusion

Data gathered from the workshop experiences provide insights into the successes and challenges of the workshop design. The TPACK Self-Reflection data indicates participants did perceive some TPACK growth during the workshop, with the least growth observed in the Content Knowledge domain, and the greatest growth in the TPACK domain. The second largest area of growth is the Pedagogical Knowledge domain, suggesting that a group of teachers representing a variety of disciplines benefited in their methods of practice through this experience.

The TPACK Self-Assessment Survey data included a 15% score increase from pre- to post-assessment, indicating a significant TPACK growth across themes. Five experienced scores which decreased, but provided notes indicating a clearer understanding of the descriptors at post-assessment. The greatest growth on this assessment was 24 points (44%), attained by two participants. This data suggests there is great potential for participants' TPACK to increase across themes (curriculum, assessment, learning, teaching, and access).

The Cyber Principles Assessment provided documentation of growth with regard to the ten principles of focus throughout the workshop. This growth is not surprising, given the amount of exploration and application dedicated to the principles throughout the week. It has been suggested that the principles be introduced in a pre-workshop format in the next iteration, which will allow more growth opportunity and a better distinction between superficial knowledge and more meaningful understanding of the principles. Further, participants were largely weak in fluency with connections of the principles to their classroom practice, suggesting that a greater amount of time should be spent on lesson development and collaboration focused on the principles within the represented content areas.

PRE-SERVICE TEACHER CURRICULUM

In the spring semester of 2018, MSU offered a special topics course to education and CS students based on AIM. The course was co-taught by faculty members from the CSE and CISE. It was co-listed on the MSU master schedule so that students could count the course either as a CS course or education course depending on the needs of their particular program. This course replaces a C language programming service course for education majors. With the traditional C programming course, no relevancy to the teaching domain for content area for each student is offered. The authors, in developing the new course, support the ideas of Yadav, et.al:

> *Embedding computational thinking in K-12 teaching and learning requires teacher educators to prepare teachers to support students' understanding of computational thinking concepts and their application to the disciplinary knowledge of each subject area. Specifically, teacher educators need to provide teachers with the content, pedagogy, and instructional strategies needed to incorporate computational thinking into their curricula and practice in meaningful ways, enabling their students to use its core concepts and dispositions to solve discipline-specific and interdisciplinary problems.*[16]

The objective of the course is to provide the background needed for the students to become successful teachers of computing and cybersecurity topics at the middle or high school level, supporting the unmet need for K-12 CS teachers in the state of Mississippi. Our hope is that providing the technical background to education students will enable them to include computing and cybersecurity topics in courses that are already part of a typical secondary education curriculum. An additional benefit of the course is prompting the CS students to investigate their opportunities in education. The course will be taught for a second time in the spring 2019 semester.

Learning Modules and Objectives

The course description is "Introduction to computer programming and cybersecurity principles in the context of classroom integration, importance of digital citizenship, computing major and career exploration, historical perspective on computing. Includes methods for teaching and evaluating." The topics that are covered include:

- History of Computing
- Block Programming (Snap!)
- Textual Programming (Python)
- Cybersecurity Fundamentals
- Current Cybersecurity Issues (Malware, Authentication, Cryptography, etc.)
- Digital Citizenship
- Adolescent Development

- K–12 Computer Science Framework
- Research Based Principles for Teaching

The mix of education and CS students in the spring 2018 offering provided a fertile ground for classroom discussions. The CS students were familiar with programming and cybersecurity, but had very limited background in adolescent development or teaching methods. The education students conversely were unexperienced in programming and cybersecurity but had more knowledge of adolescent development and teaching methods. A few of the topics (digital citizenship and the computer science framework created by the Association for Computing Machinery, Code.org, Computer Science Teachers Association, Cyber Innovation Center, and National Math and Science Initiative) were new to most of the students.

Assessment

Student assessments included programming assignments, a group presentation on an assigned cybersecurity issue, and reflection papers. The reflection papers were used both to guide students to form opinions on discussed topics and to receive student feedback on the course. One of the more interesting reflection topics asked the students whether creating programs in a block style drag and drop development environment (Snap!) was "real computer programming". We had earlier discussed that computer programs are the expression of algorithms and that algorithms are a series of instructions that the computer follows to solve a problem. Even though the programs created in Snap! are delivered as web pages and do not present the standard user interface of personal computers or mobile devices, most students did think that creating programs in Snap! is a form of programming.

Feedback from the students concerning the course was very positive. Computer science students and education students learned how to depend on each other to complete the assignments in class. Researchers examined the end-of-course surveys and focus group to determine the student views of the course. Education students stated that they found this course to be very useful and expanded their thinking on the importance of computing. All students suggested a "field trip" to the local public school campus to observe and work with students in a technology course. One unexpected suggestion was to spend more time on computer programming. Overall, the students deemed the course as very useful and encouraged the researchers to make this a permanent course in the curriculum.

In the second offering of the course in spring 2019, co-teachers and authors of this manuscript plan to use analysis of class reflections and a Q-sort to determine changes in students attitudes towards potentially seeking teacher licensure in education and formally embedding technology, CS principles and cybersecurity into mathematics and science content. Students will again be assigned reflections and a technology beliefs and self-efficacy survey will be administered. Researchers will use data to examine student change in attitude.

SUMMARY

The goal of providing opportunities for pre-service and in-service teachers to experience computing and cybersecurity is to impact their students and ultimately increase opportunities for the future workforce. To meet the needs of children across Mississippi and beyond, computer scientists and teacher educators must work collaboratively and quickly to place well-educated, confident teachers in K-12 classrooms. Developing teachers from within the current teacher workforce is necessary to build a pool of CS teachers. Likewise, creating new courses to integrate into existing teacher education programs allows us to reach pre-service teachers already in the teacher pipeline. By reaching out to teachers across a variety of disciplines and in multiple settings, the project team seeks to provide a consistent base of knowledge for teachers to use as they model in their own practice and integrate these concepts in their classroom lessons. The data suggest that teachers are growing in their TPACK through these experiences. Many of the study participants are now leading robotics clubs in their schools and integrating cybersecurity or computer programming units within their classes. This work provides promise that a collaborative effort between computer scientists and teacher educators can positively impact the classroom and promote a foundation of understanding for novice and experienced classroom teachers.

ACKNOWLEDGEMENTS

This work is funded through the generous support of the National Science Foundation INCLUDES program and the National Security Agency's GenCyber program: NSF INCLUDES 1649312, NSA H98230-17-1-0249 & H98230-17-1-0248. The authors acknowledge the contribution of Randy Lynn to content on the economic landscape in Mississippi.

REFERENCES

1. J. Ivy, S. Hollis, D. Franz, and S. Lee, "Exploring pathways to developing self-efficiency in new computer science teachers," 2017 [ASEE Zone II Conference, Puerto Rico].
2. S. Lee, L. Lineberry, J. Ivy, V. White, M. Jankun-Kelly, R. Lynn, B. Minnifield, and L. Vaughn. CodeMS: Developing Equitable Access to Computing and Cybersecurity Education in Mississippi. Submitted to 1st Annual *Conference* of *CoNECD* - Collaborative Network for Engineering and Computing Diversity. April 29 – May 2, 2018. Unpublished.
3. National Science Foundation, "10 Big Ideas for Future NSF Investments," Web. https://www.nsf.gov/about/congress/reports/nsf_big_ideas.pdf
4. C. Ashcraft and S. Blithe. 'Women in IT: The Facts,' 2010. [Online]. Available: https://www.ncwit.org/resources/women-it-facts. [Accessed : 9-Dec-2017].
5. S. Kastner, S. Lee, and T. Holifield. 'An Investigation of Pathways to Computing for Middle and High Schoolers in the U.S. South,' 2016. Proceedings of the 2016 ASEE Annual Conference & Exposition, New Orleans, Louisiana. 10.18260/p.26227.
6. L. Kaczmarczyk and R. Dopplick. 'Rebooting the Pathway to Success: Preparing Students for Computing Workforce Needs in the United States,' 2014. [Online]. Available: http://pathways.acm.org/ACM_pathways_report.pdf. [Accessed : 9-Dec-2017].
7. Mississippi Department of Education Enrollment Data. [Online]. Available: http://mdereports.mdek12.org/. [Accessed: 09-Dec-2017].
8. datacenter.kidscount.org, [Online]. [Accessed: 9-Dec-2017].
9. D. Burley, "Strengthening U.S. Cybersecurity Capabilities." *Research and Technology Subcommittee Hearing-Strengthening U.S. Cybersecurity Capabilities*. Committee on Science, Space, and Technology, 14 Feb. 2017. Web. 30 May 2017. <https://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-115-SY15-WState-DBurley-20170214.pdf>.
10. "The New England Cybersecurity Consortium: A Paradigm Shift in Education and Workforce Development in Security Fields." *ACSC Center*. Advanced Cyber Security Center, 12 Nov. 2012. Web. 30 May 2017. <https://www.acscenter.org/resources/acscwhitepaper11-12-2012.pdf>.
11. E. Sobiesk, J. Blair, G. Conti, M. Lanham, and H. Taylor, H. Cyber education: A multi-level, multi-discipline approach. *SIGITE 2015 - Proceedings of the 16Th Annual ACM Conference on Information Technology* Education, (SIGITE 2015 - Proceedings of the 16th Annual ACM Conference on Information Technology Education), 43-47. doi:10.1145/2656450.2656478
12. M. Niess, R. Ronau, K. Shafer, S. Driskell, S. Harper, C. Browning, S. Özgün-Koca, and G. Kersaint, "Mathematics teacher TPACK standards and development model," 2oo9 [Contemporary Issues in Technology and Teacher Education, 9(1).
13. M. J. Koehler and P. Mishra. "What happens when teachers design educational technology? The development of Technological Pedagogical Content Knowledge", 2005. Journal of Educational Computing Research, Vol 32 No 2, 131-152.
14. J. Ivy. "Secondary Mathematics Teachers Perceptions of Their Integration of Instructional Technologies," 2011. PhD. Thesis. The University of Mississippi.
15. J. Marshall, J. Smart, and R. Horton. "The design and validation of EQUIP: An instrument to assess inquiry-based instruction. International Journal of Science and Mathematics Education", 2010. 8. 299-321. 10.1007/s10763-009-9174-y.
16. A. Yadav, C. Stephenson, and H. Hong. "Computational Thinking for Teacher Education," 2017. Communications of the ACM, Vol 60 No 4, 55-62, 10.1145/2994591.
17. L. Lineberry, S. Lee, J. Ivy, and H. Bostick, "Bulldog Bytes: Engaging Elementary Girls with Computer Science and Cybersecurity," 2018, ASEE SE Section Annual Conference.

ABOUT THE AUTHORS

Jessica Ivy is an Assistant Professor of Mathematics and STEM Education at Bellarmine University in Louisville, Kentucky. Her research interests include the use of technology tools in teaching and STEM teacher recruitment, preparation, and retention. Ivy received her Ph.D. in Curriculum and Instruction from the University of Mississippi and is a former high school mathematics teacher. Contact her at jivy@bellarmine.edu.

Sarah Lee is Assistant Department Head and Associate Clinical Professor in Computer Science and Engineering at Mississippi State University. Her research interests include intervention strategies to increase the participation of underrepresented groups in computing majors. Lee received a PhD in Computer Science from the University of Memphis. She is a member of ASEE and ACM. Contact her at sblee@cse.msstate.edu.

Dana Franz is a Professor of Mathematics Education at Mississippi State University. Her research interests include rural teacher recruitment, preparation and retention. Franz received her Ph.D. in Education Psychology at Texas A&M University and previously taught high school mathematics and served as a curriculum coordinator. Contact her at df76@colled.msstate.edu.

Joseph Crumpton is an Assistant Clinical Professor in Computer Science and Engineering at Mississippi State University. His research interests are computer science and cybersecurity education. Crumpton received his Ph.D. in Computer Science from Mississippi State University. Contact him at crumpton@cse.msstate.edu.