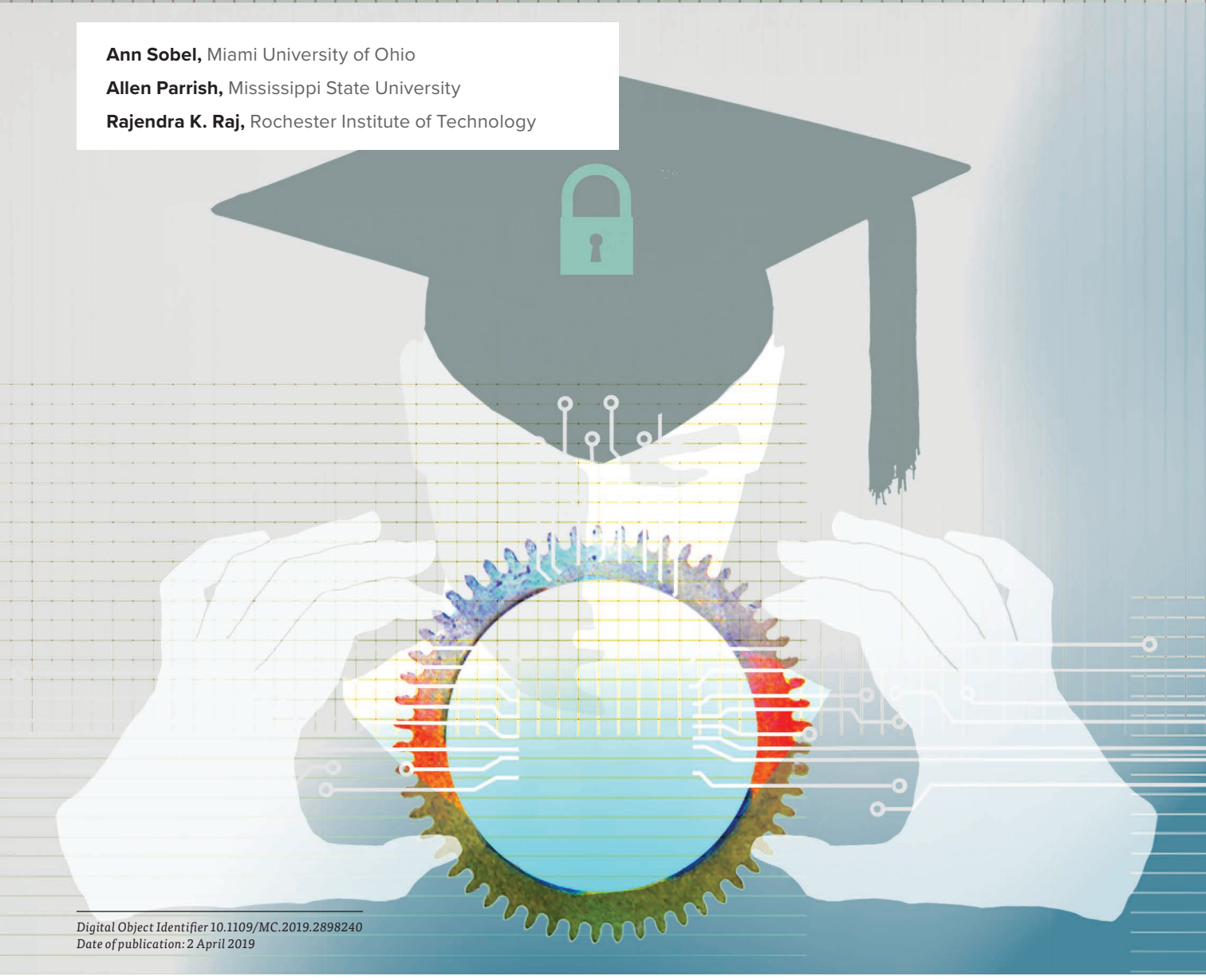
Curricular Foundations for Cybersecurity

Ann Sobel, Miami University of Ohio
Allen Parrish, Mississippi State University
Rajendra K. Raj, Rochester Institute of Technology



Digital Object Identifier 10.1109/MC.2019.2898240
Date of publication: 2 April 2019

0018-9162/19©2019IEEE

Cybersecurity has emerged at the center of several international crises, and the demand for well-educated professionals in this area has rapidly escalated. Given the newness of the area and the lack of curricular consensus about cybersecurity, education providers have struggled to keep up. More engagement is needed from the cybersecurity education community, but recent developments , such as the release of the CSEC2017 curricular guidelines, are promising.

By the end of 2019, it is expected that there may be as many as 2 million unfilled cybersecurity jobs worldwide. Education providers are working to fill this gap, and full-fledged degree programs are rapidly emerging in this area. Industry training and certification programs have also been growing rapidly as well. But even with this growth, the gap is still expected to remain large, and the diversity of skills needed within this space is substantial. Multiple pathways are needed to prepare students to engage in different types of cybersecurity jobs.

In the United States, early work in attempting to define the academic parameters of cybersecurity was performed by the National Security Agency through the National Centers of Academic Excellence (CAE) program, which was first developed and put in place in 1998. Institutions meeting the criteria established by this program are designated as CAE. This program has led the way in establishing content for cybersecurity programs and setting parameters on what a cybersecurity discipline might look like. A workforce-based effort was also led by the National Institute for Standards and Technology called *the National Initiative for Cybersecurity Education* (*NICE*). The NICE effort resulted in a workforce-based framework of seven job categories, 33 specialty areas, and 52 work roles.

The CAE and NICE programs filled a void to help define curricular expectations in a rapidly emerging area of significant national importance. But academic disciplines are both universal and peer driven, and an academic community is essential to achieve maturity. To complement these programs and help bring such a community into existence, the Cyber Education Project (CEP) was formed in 2013. CEP ultimately led to the formation of the joint task force of the Association for Computing Machinery, IEEE Computer Society, International Federation for Information Processing, and Association for Information Systems to continue the curricular exploration of cybersecurity. The joint task force developed CSEC2017, which was published in late 2017 to provide curricular guidelines for cybersecurity education. CSEC2017 builds on the content defined by the CAE program but offers a broader, more flexible view, with many different selections and arrangements of topics to reflect different emphases consistent with different types of jobs and career paths.

Using the published CSEC2017 as the basis, ABET developed accreditation criteria for undergraduate programs in cybersecurity. Programs can now apply for accreditation under these criteria. Having accreditation criteria puts cybersecurity on the same level as the more than 500 ABET-accredited undergraduate computing programs around the world. These accreditation criteria also help to define the parameters of a cybersecurity discipline, especially at the undergraduate level. If higher education is going to address cybersecurity effectively, there needs to be a common frame of reference. Not every program will be alike, but there needs to be standards and a way to compare the goals and outcomes of different types of cybersecurity degrees as well as to conduct quality assurance and continuous improvement of programs. Further, if cybersecurity is to mature as an academic discipline, there needs to be an evolving consensus of the boundaries and contents of the discipline.

The coeditors of this special issue are all involved with cybersecurity offerings at their respective universities and, as such, are all grappling with practical questions on how to define cybersecurity as an academic entity. Is cybersecurity a full-fledged discipline and degree program by itself, or should it simply be built into existing disciplines and degrees? Further, is cybersecurity a technical discipline focused on systems for securing and provisioning, is it a nontechnical discipline focused on systems that cover human factors and legal and policy contexts, or both? What aspects of cybersecurity should be part of education at the primary, secondary, undergraduate, and graduate levels? At the same time, what cybersecurity content should be offered in workforce training programs?

IN THIS ISSUE

This issue of *Computer* explores curricular foundations of cybersecurity by

ABOUT THE AUTHORS

ANN SOBEL is with Miami University of Ohio. Her current research interests include formal specification notations with an emphasis on security. Sobel received a Ph.D. from The Ohio State University, Columbus. Contact her at sobelae@miamioh.edu.

ALLEN PARRISH is with Mississippi State University. His current research interests include data science and open source intelligence gathering as well as defining the fundamentals of emerging computing disciplines, such as cybersecurity and data science. Parrish received a Ph.D. from The Ohio State University, Columbus. He is a member of the IEEE Computer Society. Contact him at allen.parrish@msstate.edu.

RAJENDRA K. RAJ is with Rochester Institute of Technology. His current research interests include data science and cybersecurity. Raj received a Ph.D. from the University of Washington, Seattle. Contact him at rkr@cs.rit.edu.

examining various pieces of the educational cybersecurity ecosystem, with the previously stated elements emphasized in different ways by various authors. As previously noted, CSEC2017 has now become the pivotal point so far in the transition from cybersecurity as a focus area driven by government and workforce demands to a bona fide academic discipline. In Hudnall's article, "Educational and Workforce Cybersecurity Frameworks: Comparing, Contrasting, and Mapping," CSEC2017 is placed into the broadest possible context by defining its role relative to both the CAE criteria and the NICE framework. Hudnall's article defines the notions of learning (CSEC2017), training (CAE), and working (NICE) as orthogonal dimensions and brings out relationships among these three frameworks. In contrast, Burley and Lewis's article, "Cybersecurity Curricula 2017 and Boeing: Linking Curricular Guidance to Professional Practice," shows how CSEC2017 can provide direct guidance in a professional setting. More experience is needed to determine the relative utility of CSEC2017 and NICE within a professional context, but Burley and Lewis establish that CSEC2017 has direct applicability within the workforce context despite the orthogonal dimensions postulated by Hudnall.

The article by Gibson and his coauthors, "Accredited Undergraduate Cybersecurity Degrees: Four Approaches," details four distinctly different models of undergraduate cybersecurity programs, all of which received accreditation in the first round of the application of the new ABET cybersecurity accreditation criteria. This reinforces the notion that cybersecurity is really a metadiscipline or a broad conglomeration of related disciplines. ABET accreditation allows all four to be accredited as cybersecurity programs, allowing diversity to emerge in how programs are implemented while still maintaining curricular standards.

One of the four ABET-accredited cybersecurity programs, the U.S. Naval Academy's Cyber Operations program, is described in depth by Emmersen and her colleagues in their article, "The USNA's Interdisciplinary Approach to Cybersecurity Education." The U.S. Naval Academy program was designed both to emphasize breadth instead of depth and promote contextualization of the technical aspects of cybersecurity within a framework of political and organizational policy as well as law. The article by Blair and her colleagues, "Educating Future Multidisciplinary

YOUR HELP IS NEEDED

We have developed a survey at https://www.surveymonkey.com/r/QZGG9B6. We need your input on how cybersecurity is viewed at your workplace. Is it considered an academic discipline or a profession? And what subject areas constitute appropriate content or expertise? We are also interested to learn what efforts related to cybersecurity are actively sought at your workplace. We invite you to complete this survey. Results will be presented in future issues of *Computer*.

Cybersecurity Teams," reinforces the U.S. Naval Academy's notion of a broad program by articulating a broad set of principles that should be part of cybersecurity programs.

Finally, in "Seeding Cybersecurity Workforce Pathways With Secondary Education," Ivy and her colleagues postulate a place for cybersecurity within K–12 education and, therefore, the compelling need to train preservice and in-service teachers to teach in this context. This integration into primary and secondary education further reinforces the idea that cybersecurity may be emerging as a bona fide academic discipline.

These articles collectively reveal the existence of markers of cybersecurity as an academic discipline: a K–12 component, model curricula, and accreditation criteria. They also show significantly different models of cybersecurity that have been successfully deployed and argue for a commitment to providing students with a broad-based educational preparation for cybersecurity careers at the postsecondary level. However, clearly, cybersecurity is an emerging discipline, and more maturation is needed before it can be concluded that a definitive foundation exists for the future in cybersecurity. With the substantial workforce demands, however, it is important that a baseline be established to start asking questions about what direction this field needs to go in for the next generation of cybersecurity programs.

Digital Object Identifier 10.1109/MC.2019.2903664