Perspectives on the Future of Cybersecurity Education

Rajendra K. Raj
Rochester Institute of Technology
Rochester, NY, USA
rajendra.k.raj@rit.edu

Joseph J. Ekstrom
Brigham Young University
Provo, UT, USA
jekstrom@byu.edu

John Impagliazzo
Hofstra University
Hempstead, NY, USA
john.impagliazzo@hofstra.edu

Steven Lingafelt
IBM
Research Triangle Park, NC
lingafel@us.ibm.com

Allen Parrish
United States Naval Academy
Annapolis, MD, USA
aparrish@usna.edu

Harry Reif
James Madison University
Harrisonburg, VA, USA
reifhl@jmu.edu

Ed Sobiesk
Army Cyber Institute
West Point, NY, USA
edward.sobiesk@usma.edu

***Abstract*—As the worldwide demand for cybersecurity-trained professionals continues to grow, the need to understand and define what cybersecurity education really means at the college or university level. Given the relative infancy of these efforts to define undergraduate cybersecurity programs, the panelists will present different perspectives on how such programs can be structured. They will then engage with the audience to explore additional viewpoints on cybersecurity, and work toward a shared understanding of undergraduate cybersecurity programs.**

Keywords—cybersecurity education; cybersecurity engineering; undergraduate computing programs; accreditation criteria.

I. Introduction

Given the continued demand for qualified cybersecurity professionals [1], different efforts have been undertaken to define the role, scope, extent and position of cybersecurity within academic disciplines in higher education. An early effort by the US Department of Homeland Security and National Security Agency to define information assurance education (now renamed cyber defense) [2], and subsequently to define cyber operations [3]. The National Initiative on Cybersecurity Education takes an approach from a different end by describing government job classifications with associated knowledge, skills and abilities [4]. A more comprehensive effort was the attemption by the Cyber Education Project to describe cybersecurity education [5], culminating in the Joint Task Force to describe curricular guidelines for cybersecurity education [6].

None of this existing work, however, defines exactly what an undergraduate cybersecurity program should contain and how such a program complements existing programs. This void will be filled by program accreditation standards [7] that should be influenced by stakeholders with international considerations from industry, military, and government.

This panel plans to address commonalities and differences in describing curricular guidelines in the cybersecurity space. The panelists will present different perspectives on cybersecurity education at the university level, and then engage with the audience to explore additional viewpoints. The intention is to develop a shared understanding of how undergraduate cybersecurity programs may be structured

II. Session Goals

The primary goals of this panel session are to:

1. Present diverse perspectives toward curriculum guidelines for high quality, four-year cybersecurity degree programs,
2. Suggest a formalization of the concept of an "undergraduate program in cybersecurity," and
3. Garner audience perspectives on the ideas presented by the panelists.

III. Panel Description

This panel focuses on presenting the perspectives of the panelists, as they relate to formalizing the notion of a "Baccalaureate in Cybersecurity." Each panelist's background and position is summarized below.

Rajendra K. Raj, a professor of computer science at RIT, focuses on the application of cybersecurity, data science and distributed computing to real-world problems, as well as on

978-1-5090-5920-1/17/$31.00 ©2017 IEEE

computing education and program accreditation. Dr. Raj co-leads the effort to revise ABET's computing accreditation criteria and develop cybersecurity criteria. He will introduce the panelists, provide the background and moderate the panel.

Joseph J. Ekstrom has three decades of software development and senior management experience, and is the former chair of BYU's Information Technology program. His research interests include network and systems management, information assurance, penetration testing and curriculum development. Dr. Ekstrom serves on the Joint Task Force on Cybersecurity Education. He will discuss accreditation criteria for cybersecurity and the requirements, if any, implied by CSEC 2017 [6].

John Impagliazzo is Professor Emeritus at Hofstra University. He was chair of the Computer Engineering Report (CE2016) steering committee, co-author of the Computing Curricula 2005 Report (CC2005), and serves of the information technology committee for IT2017. He currently serves as a consultant and expert for various countries regarding curricular, assessment, accreditation, and other related activities. He will present international perspectives in designing and institutionalizing models for cybersecurity programs.

Steven Lingafelt is a Senior Technical Staff Member with IBM Global Infrastructure. An engineer and inventor, he helped to create IBM's IT security strategy and architecture and to lead the implementation of enterprise-wide security controls and mitigation. He has also been a leader in the accreditation efforts for cybersecurity engineering, and will discuss the proposal for ABET accreditation criteria for cybersecurity engineering and the needs of technical industry as an employer/stakeholder.

Allen Parrish is Professor and Chair of the Department of Cyber Science at The United States Naval Academy, which offers the Cyber Operations degree. He previously was at the University of Alabama for over two decades, and serves on the Joint Task Force on Cybersecurity Education. Dr. Parrish co-leads the effort to revise ABET's computing accreditation criteria and develop cybersecurity criteria. He will present the need for clarity in defining different types of academic cybersecurity programs.

Harry Reif is a Professor in the College of Business and Graduate School at James Madison University, and holds visiting faculty appointments at Virginia Commonwealth University and Purdue University Graduate Schools. He has been a founder of several start-up companies in information systems and software development. Dr. Reif will utilize business and technology backgrounds to discuss the role of the business community as an employer and stakeholder of cybersecurity programs.

Edward Sobiesk is the Chief of the Education for the Army Cyber Institute, and a Professor of Computer and Cyber Science at United States Military Academy. With two decades of cyber experience as an educator, leader, and practitioner, his research interests include online privacy, usable security and computing education. He will discuss accreditation criteria for cybersecurity and the needs of the military as an employer/stakeholder.

Table I outlines the structure of the panel. Ample time is provided for audience interaction. If the audience is of sufficient size, the panelists will divide it into groups and facilitate discussions within each group, with time to report the results of the groups to the entire audience.

TABLE I. SESSION OUTLINE

	Description	**Duration (minutes)**
1.	Introductions	5
2.	Panelists' presentations	35
3.	Identification of breakout groups	5
4.	Working groups' discussions	20
5.	Working group reports	10
6.	Next Steps	5

IV. RATIONALE.

The panelists, who have diverse expertise in this space, can both inform the audience and solicit feedback from them. The session provides sufficient time for direct audience interaction to provide the needed engagement with representatives from the computing and engineering education communities. The discussions will provide multiple perspectives on cybersecurity education, which is on the frontiers of education, and should enhance the knowledge and experience of the participants.

V. AUDIENCE DESCRIPTION

The panel targets college faculty and administrators interested in incorporating cybersecurity curricular content into their programs, developing new programs, or modifying existing programs in cybersecurity. As cybersecurity education falls within both computing and engineering, this panel is likely to attract a significant portion of the typical FIE audience.

REFERENCES

[1] Bureau of Labor Statistics, U.S. Department of Labor, Occupational Outlook Handbook. 2016-17 Edition, Information Security Analysts, on the Internet at http://www.bls.gov/ooh/computer-and-information-technology/information-securityanalysts.htm, accessed: July 05, 2017.

[2] National Centers of Academic Excellence in Cyber Defense (CAE-CD) Designation Program Guidance on the Internet at https://www.iad.gov/NIETP/documents/Requirements/CAE_Program_Guidance.pdf, accessed: July 05, 2017

[3] National Centers of Academic Excellence in Cyber Operations, on the Internet at https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/criteria.shtml, accessed: July 05, 2017

[4] National Initiative for Cybersecurity Education, on the Internet at http://csrc.nist.gov/nice/framework/, accessed: July 05, 2017

[5] Cyber Education Project, on the Internet at http://www.cybereducationproject.org/ accessed: July 05, 2017.

[6] Diana L. Burley, Matt Bishop, Scott Buck, Joseph J. Ekstrom, Lynn Futcher, David Gibson, Elizabeth Hawthorne, Siddharth Kaza, Yair Levy, Herbert Mattord, and Allen Parrish, Cybersecurity Curricula 2017, Version 0.75 Report, 12 June 2017. on the Internet at https://www.csec2017.org/, accessed: July 05, 2017.

[7] ABET, on the Internet at https://www.abet.org/, accessed: July 05, 2017.