Chapter 5
Improving Cyber Defense Education Through National Standard Alignment: Case Studies

Ping Wang
Robert Morris University, USA

Maurice Dawson
Illinois Institute of Technology, USA

Kenneth L Williams
American Public University System, USA

ABSTRACT

There has been a fast-growing demand for cybersecurity professionals to defend cyber space and information systems. With more and more programs and course offerings in cybersecurity popping up in higher education, it is important to have a consistent and reliable quality standard to guide and evaluate the training and preparation of qualified cyber defense workforce. The national Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) designation program jointly sponsored by the US National Security Agency (NSA) and Department of Homeland Security (DHS) is a rigorous national standard with specific criteria for maintaining the quality of cybersecurity education. This article explains the CAE-CDE program criteria and requirements and discusses the important role of the special designation in improving cyber defense education and workforce development. This article illustrates the educational value and quality impact of the CAE-CDE program with three case studies: (1) University of Missouri – St. Louis; (2) American Public University; and (3) Robert Morris University.

DOI: 10.4018/978-1-5225-7912-0.ch005

1. INTRODUCTION

This paper uses case studies to explore the important topic of how to improve the quality of cyber defense education in the United States through national standard alignment. Cyber defense is the core aspect of Cybersecurity, which has been a fast-growing career field and an important area with increasing demand and opportunities for higher education. Information security analyst is only one of the cybersecurity career titles. According to U.S. Department of Labor Bureau of Labor Statistics (BLS), employment of information security analysts is projected to grow 28% from 2016 to 2026, much faster than the average growth rates of 7% for all occupations and 13% for all computer related occupations (U.S. Department of Labor, 2018).

The latest cybersecurity workforce framework published by the National Initiative for Cybersecurity Education (NICE) recognizes the growing need for an integrated cybersecurity workforce with technical and non-technical roles for organizations to address their cybersecurity challenges and implement their missions and business processes connected to cyberspace. The NICE Cybersecurity Workforce Framework (NCWF) emphasizes that "academic institutions are a critical part of preparing and educating the cybersecurity workforce" (National Initiative for Cybersecurity Education, 2017). A recent study shows that top U.S. universities were failing at cybersecurity education with a lack of cybersecurity requirements for graduates and a slow change in curriculum and courses (White, 2016). However, it is encouraging to see more and more 2-year and 4-year academic institutions have started to offer cybersecurity degree programs and courses across the country. Quality assurance is needed for cybersecurity-related degree programs to meet high cybersecurity academic standards in order to prepare the graduates for the growing number of cybersecurity positions (National Initiative for Cybersecurity Careers and Studies, 2017).

The national Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) designation program jointly sponsored by the US National Security Agency (NSA) and Department of Homeland Security (DHS) is a national quality standard for certifying and maintaining high quality of cybersecurity education with rigorous and consistent requirements for program evaluation and close alignment to specific cybersecurity knowledge units. Out of over 5300 colleges and universities in the U.S., only about 200 of them have achieved the CAE-CDE designation status. Attendance at a CAE school will give students confidence in learning, and a degree from a CAE school will give employers confidence in hiring (National Initiative for Cybersecurity Careers and Studies, 2017).

This paper will describe the background for CAE-CDE program, highlight the important application and designation criteria, and use the case study methodology to present three different cases of academic institutions with different CAE status: University of Missouri – St. Louis (UMSL), American Public University System (APUS), and Robert Morris University (RMU). The goal of the study is to illustrate the important role of the CAE designation and the application process in improving the quality of cybersecurity education and workforce preparation at these institutions through alignment of a national standard for quality control.

2. BACKGROUND

The national CAE-CDE program evolved from the initial national CAE in Information Assurance Education (CAE-IAE) program started by NSA in 1998 with DHS joining as a co-sponsor in 2004, and the CAE in IA Research special designation was added in 2008 to encourage doctoral level research in cybersecurity