Reflections on Applying for CAE-CDE Designation

Ulku Clark
clarku@uncw.edu
Information Systems

Geoff Stoker
stokerg@uncw.edu
Computer Science

University of North Carolina Wilmington
Wilmington, NC 28403

Abstract

The increase in importance of cybersecurity in general and the rise of cybercrime in particular provide strong justification for continued support of the National Security Agency (NSA) and Department of Homeland Security (DHS) jointly sponsored program for National Centers of Academic Excellence in Cyber Defense Education (CAE-CDE). This paper motivates the need for the continued existence of programs like CAE-CDE and describes our recent experience in applying for this designation.

Keywords: Cybersecurity, Centers of Academic Excellence, CAE, Knowledge Units

1. INTRODUCTION

According to Juniper Research, the cost of cybercrime is estimated to exceed $8 trillion globally by 2022 (Moar, 2017). North American breaches are projected to account for about 60% of all the data breaches, or $4.8 trillion, which is greater than most countries' GDPs. The steady annual increase of criminal breach incidents and state sponsored hacking are the main drivers of the dramatic increase of the cost estimates. There have been numerous high-profile incidents in the recent past, but perhaps the most high-profile recent state sponsored hacking incident is related to the 2016 US presidential election (Vincent, 2017). The state-sponsored hackers managed to gain unauthorized access to sensitive data through vulnerability exploitation and quite possibly influenced the election. Two years after the election the issues caused by this incident are still being investigated.

In addition, state mandated digitization of records in most industries (e.g. HIPAA), the growing adoption of the Internet of Things (IoT), and wearable devices create unforeseen vulnerabilities that are often exposed by hackers. Even though digitization of records offers a wonderful array of conveniences (easy sharing of records, reducing costs, etc.), many of the organizations (especially small and medium sized businesses) do not have the capabilities to secure the digitized records beyond the required minimum (examples of the practice guides can be found at National Institute of Standards and Technology (NIST) - Cybersecurity Practice Guides), and in most cases the baselines are vaguely implemented leaving the records wide open for unauthorized access by anyone with even an intermediate grasp of offensive information security knowledge – a recent DefCon demonstration of how easily police bodycams can be hacked (Newman, 2018). IoT devices like thermostats or digital cameras are open for exploit unless secured. In 2016 the IoT Mirai

Botnet affected huge portions of the Internet, including Netflix and CNN (Kolias, et.al., 2017). In January 2018, it was revealed that the fitness trackers used by US military personnel (though not issued by the US military) were tracking them and creating a vulnerability by uploading the data to a heat map that could disclose classified locations and routes. The vulnerabilities exploited by hackers also significantly increased the number of ransomware cases, such as WannaCry which crippled services within hospitals and other facilities in the United Kingdom, and NotPetya which hindered Ukrainian infrastructure such as the power grid, airports, and public transit (Greenberg, 2018; Newman, 2017).

This growing cost caused by cybercrime leads to an increase in demand for cybersecurity professionals. The Bureau of Labor Statistics reports a 28% growth expectation in information security analysts demand from 2016 to 2026. The field is currently overwhelmingly lacking a sufficient number of trained professionals to meet the demand. The (ISC)2 survey conducted in 2015 states that by 2022 the cyber security workforce gap is to reach 1.5 million – this forecast is updated to 1.8 million two years after the report was released due to the recent events and shifting industry dynamics ((ISC)2, 2017)). In 2017 more than 350,000 US cybersecurity jobs were unfilled. The Information Systems Audit and Control Association's (ISACA) "State of Cybersecurity: Implications for 2016" survey results of 461 cybersecurity managers and practitioners from around the globe show that 33% of respondents felt that, on average, less than 25% of cybersecurity applicants were qualified upon hire; while an additional 27% of respondents felt that 1 of every 2 new hires was not qualified. In addition, the security practitioners' ability to understand business and communication are reported by the security managers to be the most significant skill gap followed by the technical skills. A cybersecurity team could need a vast array of skills. Some of these skills require a good amount of experience and only a very finite pool of professionals possess them. At the moment, even the entry level skills are in high demand. However, the entry level jobs also require some hands-on experience.

Nationwide there are several initiatives to alleviate the supply issue. Before the accreditation agencies, such as the Association for Computing Machinery (ACM), had the chance to develop curricular guidelines, many higher education institutions had to step up and started offering classes, certificates or undergraduate and/or graduate degrees on cybersecurity topics based on their understanding of the nation's needs. The US government recognizes the potential threat of cyber-attacks on vital components of the country's Supervisory Control and Data Acquisition (SCADA) networks, which are systems performing key functions in providing essential services and commodities (e.g., electricity, water, transportation), and the need for a skilled workforce to combat the risks. Consequently, there has been a substantial effort by the National Security Agency (NSA) and Department of Homeland Security (DHS) to support the academic entities building the needed workforce through their Center of Academic Excellence (CAE) designation. The NSA/DHS CAE program will be discussed in detail later in the paper.

In parallel with the government efforts, the ACM recently released Cybersecurity Curricula (CSEC) 2017 to provide curricular recommendations in cybersecurity education (CSEC 2017). The ACM guidelines were drafted by a Joint Task Force (JTF) on Cybersecurity Education that was comprised of professional and scientific computing groups and/or societies such as the ACM, Institute of Electrical and Electronics Engineers Computer Society (IEEE CS), Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and the International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). The JTF used Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science, Global IT Skills Framework for the Information Age (SFIA), requirements of the NSA/DHS CAE in Cyber Defense and Cyber Operations, Information Technology Curricula 2017: Curriculum Guidelines for Baccalaureate Degree Programs in Information Technology, Guide to the Systems Engineering Body of Knowledge, and US National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework as the major resources in the development of the guidelines.

While many higher education institutions are in the process of adopting the ACM guidelines that are in agreement with CAE requirements, currently in the US the curricula followed by NSA/DHS CAE designated schools have the benefit of having gone through an objective outside review and, among some recruiters, have added credibility. This paper focuses on the CAE designation given jointly by the NSA and DHS to higher education institutions to promote education in cybersecurity. This paper aims to

provide insights to educators on what the designation is, what the requirements to get the designation are, and recommends a timeline for prospective applicants.

2. CENTERS OF ACADEMIC EXCELLENCE (CAE) PROGRAM

Brief History

The National Security Telecommunications and Information Systems Security Committee (NSTISSC) was established in 1990 to provide a forum for the discussion of policy issues and to provide operational guidance for the protection of national security systems (Report of the President, 2001). Among other things, the NSTISSC established training standards that formed the basis for criteria used to evaluate the strength and maturity of educational institutions' information assurance and information systems security (INFOSEC) curricula. In 1998, the NSA created the National INFOSEC Education and Training Program (NIETP) [1] to offer a variety of products and services in IA/INFOSEC education and training, including the sponsorship of the Academic Centers of Academic Excellence in Information Assurance Education (CAE-IAE). After the first round of applications, seven centers in five states were designated in 1999 as CAE-IAE: James Madison University, George Mason University, Idaho State University, Iowa State University, Purdue University, University of California at Davis, and University of Idaho (Bishop & Taylor, 2009). In 2004 the DHS joined on as a partner with the NSA in sponsoring CAEs. The CAE in IA Research was added in 2008 and in 2010, the CAE-2Y was established to allow two-year institutions to receive the CAE designation.

Centers of Academic Excellence in Cyber Defense Education (CAE-CDE)

Jointly sponsored by NSA and DHS, the National CAE-CDE program has the stated goal, "to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense (CD) and producing a growing number of professionals with CD expertise in various disciplines." CAE-CDE designated schools are formally recognized by the US Government as meeting high, objective standards for CD education. Students at CAE-CDE institutions are eligible to apply for certain scholarships and grants including the Federal Cyber Service Scholarship for Service program.

Regionally accredited two-year institutions can apply for designation as a CAE in Cyber Defense Two-Year Education (CAE-2Y). Four-year colleges, graduate-level institutions, and Department of Defense (DoD) schools can apply to be designated as a CAE in Cyber Defense Education (CAE-CDE), a CAE in Cyber Defense Research (CAE-R), or potentially both. Twenty years after the designation of the first seven CAE-IAE (as of June 2018), there are 240 additional institutions now designated as NSA/DHS National CAE in Cyber Defense in 48 states [2], the District of Columbia, and Puerto Rico listed on the NIETP website ("National IA Education & Training Programs", n.d.). The breakout by CAE designation is in table 1. This represents about 5% of eligible higher education institutions.

Applying for CAE-CD designation involves meeting two overarching sets of criteria: program requirements and mapping curricula to cyber defense knowledge units (KUs). The NIETP website provides the functionality for creating an institution account and submitting all required information.

CAE Designation	# of Institutions
CAE-2Y	64
CAE-CD	111
CAE-R	29
Both CAE-CD / -R	43

Table 1 – CAE designation by type and number of institutions.

Program Requirements

There are some minor differences in the details of the program requirements for CAE-2Y and CAE-CD designation, but the 8 requirement areas are the same. In table 2, we provide a high-level description of the program requirements. The detailed requirements for both CAE-2Y and CAE-CD are available on the NIETP website ("National IA Education & Training Programs", n.d.) in two detailed .pdf documents.

Program requirement
0. Letter signed by the Provost or higher that provides official notice of institutional endorsement and intent to participate in the CAE-CDE program.
1. Evidence that the cyber defense academic curriculum path has been in existence for at least three years with one year of student granted degrees with path completion.
2. Evidence that the institution fosters student development and assessment in the field of Cyber Defense.
3. "Center" for Cyber Education - proof that the institution has an officially established entity (physical or virtual) serving as the

focal point for cyber curriculum and practice.
4. Evidence of sufficient cyber faculty to ensure continuity of the cyber defense program.
5. Evidence that cyber defense is a multidisciplinary practice that is integrated into additional degree programs within the institution.
6. Institution security plan that includes the policies and practices used to protect the information systems infrastructure.
7. Evidence of cyber outreach/collaboration beyond the institution.

Table 2 – program requirements for CAE designation.

Curricula Requirements

As of the spring of 2018, applying for CAE-CD required successful mapping of some portion of an institution's curriculum to all 11 of the two-year core KUs, all 6 of the four-year core KUs, and any 5 of the 51 optional KUs. (NOTE: for fall 2018 there are some significant changes that differ from the KU mapping presented here; the general process appears to remain the same.)

The process of mapping institution curricula to KUs first involves identifying institution courses that cover the topics and meet the objectives for the KUs. The NIETP website provides a useful mapping matrix Excel spreadsheet for this purpose. Once courses have been identified, information and meta data for each course intended to be mapped can be entered on the NIETP website. Meta data includes items like course length, current/past enrollment, and course creation date. Information includes items like a syllabus, outline, major topics, major topic descriptions, and objectives.

When courses intended for mapping are completely input to the NIETP website, the process of mapping courses to KUs can be completed. (NOTE: all courses do not have to be completely submitted before mapping to KUs can begin.) Every KU topic must be mapped to at least one supporting course's major topics and course objectives. Each KU Outcome must be mapped to applicable course major topics and course objectives, as well as provided a paragraph of justification.

As an example of the details involved with each KU, the definition, topics, and outcomes provided with the two-year core KU, Network Defense, are provided in table 3.

The mapping process for this KU involves identifying at least one course, a major topic, and a course objective for each of the topics in the KU. For example, the topic "Network Monitoring" was mapped to our course, *MIS320 – Network Fundamentals*. The major topic mapping was to Lesson 3 – Network Protocols and Communications and the mapped MIS320 objective was "Examine the OSI and TCP/IP layers in detail to understand their functions and services."

For KU outcomes, in addition to mapping major topics and course objectives, there is a justification requirement. For the outcome listed in table 3, we provided: "Students use wireshark and packet tracer to monitor network traffic."

The 11 two-year core KUs and 6 four-year core KUs required to be mapped to institution courses are listed in table 4.

Definition – The intent of this Knowledge Unit is to teach students the techniques that can be taken to protect a network and communication assets from cyber threats.
Topic(s): Implementing IDS/IPS Implementing Firewalls and VPNs Defense in Depth Honeypots and Honeynets Network Monitoring Network Traffic Analysis Minimizing Exposure (Attack Surface and Vectors) Network Access Control (internal and external) DMZs / Proxy Servers Network Hardening Mission Assurance Network Policy Development and Enforcement Network Operational Procedures Network Attacks (e.g., session hijacking, Man-in-the-Middle)
Outcome(s): Students will be able to: Describe the various concepts in network defense. Apply their knowledge to implement network defense measures. Use a network monitoring tool (e.g., WireShark). Use a network mapping tool (e.g., Nmap).

Table 3 – elements of the two-year core KU, IT System Components

In addition to the 17 required KUs, we had to select 5 optional KUs for the program path and chose:

IA Compliance
IA Standards
Independent Study
Network Security Administration
Operating Systems Hardening

Our initial efforts mapping institution courses to KUs resulted in 14 courses being considered for the certification path. As we worked through the details of entering course information on the NIETP website and mapping courses to KUs, we determined that the mapping could be done more efficiently with 11 courses. The full mapping we did is provided in figure A1 in the appendix.

Spring 2018 (and earlier)
Core 2Y KUs
Basic Data Analysis
Basic Scripting
Cyber Defense
Cyber Threats
Fundamental Security Design Principles
Information Assurance Fundamentals
Introduction to Cryptography
Information Technology System Components
Networking Concepts
Policy, Legal, Ethics and Compliance
Systems Administration
Core 4Y KUs
Databases
Network Defense
Network Technology and Protocols
Operating Systems Concepts
Probability and Statistics
Programming

Table 4 – Core 2Y and 4Y KUs

We are aware from a few others who went through this process that it is common to pare down the number of courses used for mapping. For example, in the Darabi and Cruz paper (2015), the authors indicate they started with 62 mapped courses and ended up using 20. One of the key reasons they point out for having a manageable number of courses is that only students who take all path courses are eligible for recognition at graduation.

3. RECOMMENDATIONS

We started the most recent effort to seek CAE-CDE designation about 6 months before the submission deadline. This was only possible because one of the authors had attempted to pursue designation several years ago, but for several reasons, including lack of support, that first bid fell flat. Applying for designation is not a small undertaking. Schweitzer, et al, (2006) provide an account of an institution that committed to applying for CAE designation 3 years before doing so in order to ensure all requirements could be satisfactorily met. Darabi and Cruz (2015) indicate they worked about 6 months in preparation for applying for re-designation.

In light of our first attempt and our most recent (hopefully successful) attempt, we have 4 suggestions for those considering seeking CAE designation.

Suggestion 1 – Get buy-in.
You are going to need a letter signed by at least the Provost endorsing the effort, but the point is you will need a lot of support both vertically and horizontally to meet the program requirements and to assemble required evidence that your curriculum covers all necessary KUs. If your leadership from department up through the institution levels are not on board, you are going to have a very difficult time applying for designation.

Suggestion 2 – Do a mapping of courses to KUs early.
Depending on your confidence level of course-to-KU coverage, you may want to do a rough mapping of courses to KUs even before you approach the academic leadership hierarchy for buy-in; this will depend on your particular situation. Once you are committed to seeking designation, you will definitely want to do a thorough mapping of courses to KUs as a first step. Use the Excel spreadsheet provided; it is well constructed. This activity will reveal any gaps or excessive overlaps in the courses you intuitively choose for initial mapping. It will also help to identify early those among the faculty to whom you will be going for support while gathering and submitting the required mapping evidence.

Suggestion 3 – Participate in the mentor program.
A key aspect of the CAE-CDE program now that did not seem to exist several years ago when we first considered applying for designation is the availability of mentors. While it is likely that differing personalities will cause various mentees' experiences to vary, our personal experience with our assigned mentor was so positive and obviously helpful that taking advantage should be a no-brainer.

Suggestion 4 – Provide primary personnel with sufficient time.

This suggestion ties in with suggestion 1. Whereas with the first attempt, one of the authors tried to apply while conducting "business as usual," the second time around, both authors were given a course drop during the spring semester leading up to the application deadline. With the amount of work required, it does not seem likely that the application process could have been completed if the institution leadership had not supported that action.

4. CONCLUSIONS

With our world becoming more digital every day and with bad actors proliferating in cyberspace, the need to produce professionals with cyber defense expertise will grow for the foreseeable future. The CAE-CDE program is a vital part of the process of setting cyber defense curriculum standards and fostering a community of like-minded educational institutions. In this paper we have shared our recent experience applying for CAE-CD designation which we hope will inspire and assist others considering doing the same. We hope our description and brief analysis will assist not only those applying for the first time, but also those schools who will be coming up for re-designation.

5. ACKNOWLEDGEMENTS

We would like to acknowledge our CAE-CDE Program mentor, Nelbert (Doc) St. Clair, for his invaluable support in guiding us through the application process.

6. ENDNOTES

[1] NIETP is an overloaded acronym; also used for National Information Assurance (IA) Education and Training Program.

[2] North Dakota and Wyoming do not yet have CAE designated institutions.

7. REFERENCES

Bishop, M., & Taylor, C. (2009). A Critical Analysis of the Centers of Academic Excellence Program. Proceedings of the 13th Colloquium for Information Systems Security Education (CISSE).

CSEC 2017 https://www.csec2017.org/

Darabi, D. & Cruz, A. 2015. Meeting the CAE IA/CD Knowledge Units Requirements for the Polytechnic University of Puerto Rico. 13th LACCEI Annual International Conference.

Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

(ISC)2 (2017). 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk. https://iamcybersafe.org/wp-content/uploads/2017/07/N-America-GISWS-Report.pdf

Kolias, C., Kambourakis, G., Stavrou, A. (2017). DDoS in the IoT: Mirai and Other Botnets. Computer. V.50, issue 7, pp. 80-84.

Moar, J. (2017) The Future of Cybercrime & Security: Threat Analytics, Impact Assessment & Leading Vendors 2018-2023. Hampshire, UK. Juniper Research.

National IA Education & Training Programs. (n.d.). Retrieved from https://www.iad.gov/NIETP/index.cfm.

National Institute of Standards and Technology (NIST), National Cybersecurity Center of Excellence: https://www.nccoe.nist.gov/

Newman, L.H. (2017). How an accidental 'kill switch' slowed Friday's massive ransomware attack. https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/

Newman, L.H. (2018). Police Bodycams Can Be Hacked to Doctor Footage. https://www.wired.com/story/police-body-camera-vulnerabilities/

Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities. (2001).

Schweitzer, D., Humphries, J., & Baird, L. 2006. Meeting the Criteria for a Center of Academic Excellence (CAE) in Information Assurance Education. Consortium for Computing Sciences in Colleges.

Vincent, A. (2017). State-sponsored hackers: the new normal for business. Network Security. Volume 2017, Issue 9, September 2017, Pages 10-12.

ISSN: 2473-3857
v4 n4630

Appendix A

	CIT110 Fluency in Information Technology	CIT225 Platform Technologies	CSC131 Introduction to Computer Science	CSC385 Professional and Ethical Issues in Computer Science	MIS315 Management of Database Systems	MIS316 Business Application Development	MIS320 Network Fundamentals	MIS324 Information Security and Assurance	MIS352 Network System Administration	MIS365 Ethical Hacking	STT215 Introduction to Statistics
Basic Data Analysis											x
Basic Scripting		x	x								
Cyber Defense								x	x	x	
Cyber Threats								x		x	
Fundamental Security Design Principles								x	x	x	
Information Assurance Fundamentals	x							x		x	
Introduction to Cryptography								x		x	
Information Technology System Components							x	x	x		
Networking Concepts							x	x			
Policy. Legal, Ethics and Compliance				x				x		x	
Systems Administration											
Databases					x			x		x	
Network Defense							x	x		x	
Network Technology and Protocols							x		x		
Operating Systems Concepts		x							x		
Probability and Statistics											x
Programming			x								
IA Compliance	x			x				x			
IA Standards	x			x				x			
Independent Study										x	
Network Security Administration							x	x		x	
Operating Systems Hardening		x							x	x	

Figure A1 – mapping of UNCW courses to mandatory and optional KUs for spring 2018