Looking Ahead to CAE-CD Program Changes

Ulku Clark
clarku@uncw.edu
Information Systems

Geoff Stoker
stokerg@uncw.edu
Computer Science

Ron Vetter
vetterr@uncw.edu
Computer Science

University of North Carolina Wilmington
North Carolina, NC

Abstract

The rising number and cost of cybersecurity attacks justifies continued strong interest in the National Security Agency (NSA) and Department of Homeland Security (DHS) jointly sponsored program for National Centers of Academic Excellence in Cyber Defense (CAE-CD). After briefly outlining the current state of the cybersecurity challenge, this article describes our recent experience in successfully applying for designation as a CAE in 2018 and looks ahead to the considerable program changes in effect with the 2019 CAE-CD application. Those seeking CAE re-designation will be interested to know that there is an estimated 19% increase in required mappings as the previous mandatory Knowledge Units (KU) are replaced with the new foundational + technical core KU path. And, with the creation of a new non-technical path, an institution interested in adding that path will find 35% of the required mapping work will be new.

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

1. INTRODUCTION

According to Juniper Research, the cost of cybercrime will exceed $8 trillion globally for the 5-year period 2017-2022 (Moar, 2017). The steady annual increase of criminal incidents and state sponsored hacking are the main drivers of the dramatic increase of the cost estimates. The most high-profile state-sponsored hacking incident to date is related to the 2016 US presidential election (Vincent, 2017). The hackers managed to gain unauthorized access to sensitive data through vulnerability exploitation and quite possibly influenced the election.

In addition, state-mandated digitization of records in most industries (e.g. HIPAA), the growing adoption of the Internet of Things (IoT), and the proliferation of network-capable wearable devices create unforeseen vulnerabilities that are often exposed by hackers. Even though digitization of records offers numerous 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, and in most cases the baselines are

vaguely implemented leaving the records open for unauthorized access by anyone with even an intermediate grasp of offensive information security knowledge. 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 from 2016 to 2026. The (ISC)2 survey conducted in 2017 states that by 2022 the cybersecurity workforce gap will reach 1.8 million ((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: 2019" survey results of 1,020 cybersecurity managers and practitioners from around the globe show that 30% of respondents felt that, on average, less than 50% of applicants to open cybersecurity positions were qualified; while an additional 29% of respondents felt that 3 of every 4 new hires were not qualified.

Nationwide there are several initiatives to alleviate the supply issue. Before the accreditation agencies (e.g. the Accreditation Board for Engineering and Technology (ABET) or the Association to Advance Collegiate Schools of Business (AACSB)) or professional societies (e.g. the Association for Computing Machinery (ACM) or the Institute of Electrical and Electronics Engineers (IEEE)), had the chance to develop curricular guidelines, many higher education institutions had to step up and start 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 NSA and DHS to support the academic entities building the needed workforce through their CAE designation.

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, IEEE Computer Society, 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-CD designated schools have the benefit of having gone through an objective outside review and, among some recruiters, have added credibility. This article focuses on the CAE-CD related designations and aims to provide insights to educators on what the designation is, what the requirements to get the designation are, and provides some recommendations 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) 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 sponsoring partner. The CAE in IA Research was added in 2008 and the CAE-2Y, for designating two-year institutions, in 2010.

Centers of Academic Excellence in Cyber Defense (CAE-CD)

NSA sponsors two types of CAE: one in Cyber Defense (CD) and one in Cyber Operations (CO). In this article, we address CAE-CD programs. The NSA/DHS National CAE-CD program has the stated goal, "to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise." CAE-CD designated schools are formally recognized by the US Government as meeting high, objective standards for CD education.

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, there are 297 institutions designated (September 2019) as NSA/DHS National CAE-CDE in 48 states [Alaska and Wyoming do not currently have CAE-CD designated institutions.], the District of Columbia, and Puerto Rico listed on the NIETP website ("National IA Education & Training Programs", n.d.). The breakout is: 97, CAE-2Y; 124, CAE-CDE; 28, CAE-R; and 48, both CAE-CDE/CAE-R. This represents about 6.9% of eligible higher education institutions.

Program Requirements

The university mentioned in this paper is serving ~14,500 undergrads and 2,200+ graduate students. The program mapped to the CAE-CDE Knowledge Units (KU) is the BS in Information Technology (IT) with CyberSecurity Minor. The IT program is an interdisciplinary degree offered by the business school and the College of Arts and Sciences. The CAE-CD program description, experience, and recommendations in this section reflect our successful application for accreditation in spring 2018. The next section will highlight noteworthy differences in effect for applicants of CAE-CD designation in 2019 and beyond.

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.

There are some minor differences in the details of the program requirements for CAE-2Y and CAE-CDE designation, but the 8 requirement areas are the same. The requirements for both are available on the NIETP website. At a high level, the program requirements are:

0. Letter signed by the Provost or higher that provides official notice of institutional endorsement and intent to participate in the CAE-CD program.
1. Evidence that the CD 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 of an official institution 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 CD program.
5. Evidence that CD 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.

Curricula Requirements

In spring 2018, applying for CAE-CDE required successful mapping of an institution's CD curriculum path 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.

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 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 all information and meta data for a course intended for mapping is input to the NIETP website, the mapping to relevant KUs can be done. 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, and provided a justification.

For example, here are the details related to the four-year core KU, *Network Defense*:

Definition – The intent of this KU 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).

To map KU Topics, you must identify at least one course, a major topic, and a course objective. We mapped the topic "Network Monitoring" to our course, Network Fundamentals; the major topic, Lesson 3 – Network Protocols and Communications; and the course objective, "Examine the OSI and TCP/IP layers in detail to understand their functions and services."

For KU outcomes, in addition to mapping courses, major topics, and course objectives, there is a justification requirement. For the outcome, "Students will be able to use a network monitoring tool," our justification was: "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 the left side of table 1 (found in the Appendix), which also provides a listing that shows the required and optional KUs for both spring 2018 (and earlier) and fall 2018 side-by-side for ease of comparison. While there is a fair amount of overlap between the KU sets, those familiar with the previous mapping process will find that there is also a non-trivial amount of change.

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

Even though our initial efforts mapping institution courses to KUs resulted in 14 courses being considered for the certification path, we determined that the mapping could be done more efficiently with 11 courses. We found that it is common to pare down the number of courses used for mapping. For example, Darabi and Cruz (2015) started with 62 mapped courses and ended up using 20 to have a manageable number of courses as students need to take all path courses to be eligible for recognition at graduation. The full mapping we did is provided in table 2 (found in the Appendix).

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 second most recent 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. As well, it is worth noting that one of the faculty members working full time on this application was from the business school and the other one was from the college of arts and sciences. This arrangement ensured the curricular requirements of both disciplines involved in offering the interdisciplinary IT degree were represented and addressed.

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. 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-CD 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. The CAE designation rate increased from 42% to 92% since the mentorship program was launched in 2016 (Chan et. al. 2017).

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, tow of the authors were given a course release 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. CHANGES TO CAE

Under the new structure, the CAE-CD program types are aligned by degree: Associates, Bachelors, Masters, or Doctoral. The program requirements enumerated earlier are essentially the same, but there are noticeable changes with the KU mapping. For the Associates and Bachelors programs, institutions still need to provide mappings from program path courses to the mandatory (foundational and core) KUs. Masters and Doctoral programs have the choice of either providing a mapping from their program of study to the mandatory KUs or, if foundational and core knowledge are prerequisites for admission to the graduate program, demonstrating that admitted students possess the necessary knowledge. One way this could presumably be accomplished is by stipulating that matriculating students come from a Bachelors program that was CAE designated. All program types must provide a mapping from the optional KUs to the program of study.

Figure 1 (found in the Appendix) is provided in the "CAE-CD 2019 Knowledge Units" document available on the NIETP website. It provides a visual representation of the possible program paths at each degree level and how those paths interact with the Foundational KUs, Technical

Core KUs, Non-Technical Core KUs, and Optional KUs.

Another change with the new structure is that there are now two program paths available for each program type: technical and non-technical. All paths must include the same foundational KUs, but there are now two different five-KU sets representing core knowledge.
The new group of mandatory KUs (Foundational KUs, Technical Core KUs, and Non-Technical Core KUs) derive their topics and outcomes from a mixture of the previous Core 2Y KUs, Core 4Y KUs, Optional KUs, and new items. As a high-level indication of the scope of change, note that the previously required Core 2Y KU, *Basic Data Analysis*, and Core 4Y KU, *Probability and Statistics* have both been removed. As well, the KU *Basic Scripting* and the KU *Programming* have been merged. We provide a summary listing in table 3.

In an effort to provide a sense of the scope of work involved with the change, we indicate the number of objectives and topics, as well as how many are new – meaning those topics or objectives did not previously exist in the KUs (mandatory or optional) prior to fall 2018. For example, Cybersecurity Functions (CSF) shows: [O:5(1), T:17(2)]. This shorthand is meant to convey there are 5 objectives for this KU, 1 of which is new; and there are 17 topics, 2 of which are new. The numbers in parentheses should sum to the number of "new items" indicated. The objectives and topics not identified as "new" were drawn from the old KUs enumerated below the shorthand.

For institutions awarding Associates and Bachelors as currently designated CAE-2Y or CAE-CDE schools, the new KU structure is the same in overall number of KUs (11 for CAE-2Y/Associates and 22 for CAE-CDE/Bachelors); however there are some differences in what KUs are required and in the make-up of some of the new, mandatory KUs. The new foundational + technical core KU path most closely resembles the old 2Y/4Y mandatory KUs. Comparing the outcomes and topics across structures, we found that about 19% of the required mappings are new; meaning, they weren't previously listed as part of the old mandatory KUs.

With the creation of a new non-technical path to CAE designation, there will be some new work for any previously designated CAE to add this track.

Technical Core KUs
Basic Cryptography (BCY): [O:4, T:18(3)] – 3 new items Introduction to Cryptography
Basic Networking (BNW): [O:6(1), T:9] – 1 new item Network Concepts Network Defense
Basic Scripting and Programming (BSP): [O:4, T:13(3)] – 3 new items Basic Scripting Programming
Network Defense (NDF): [O:4(3), T:13] – 3 new items Network Defense
Non-Technical Core KUs
Cyber Threats (CTH): [O:2, T:18(1)] – 1 new item Cyber Threats
Cybersecurity Planning and Management (CPM): [O:12(7), T:9] – 7 new items Cybersecurity Planning and Management (previously optional KU)
Policy, Legal, Ethics, and Compliance (PLE): [O:3, T:10] Policy, Legal, Ethics, and Compliance
Security Program Management (SPM): [O:3, T:17(6)] – 6 new items Security Program Management (previously optional KU) Cybersecurity Planning and Management (previously optional KU) Systems Certification and Accreditation (previously optional KU)
Security Risk Analysis (SRA): [O:5, T:7] Security Risk Analysis (previously optional KU)
Foundational KUs
Cybersecurity Functions (CSF): *[O:5(1), T:17(2)] – 3 new items* *Information Assurance Fundamentals* *Cyber Defense* *Cyber Threats* *Introduction to Cryptography* *Policy, Legal, Ethics, and Compliance*
CyberSecurity Principles (CSP): *[O:5, T:15(2)] – 2 new items* *Fundamental Security Design Principles* *Cyber Defense*
IT Systems Components (ISC): *[O:4(3), T:19(8)] – 11 new items* *IT System Components* *Systems Administration* *Networking Concepts* *Cyber Defense* *Cyber Threats*

Table 3 – enumeration of Foundational, Core Technical and Core Non-technical KUs, and the pre-fall 2018 KUs from which objectives and topics are derived

If a current CAE designated institution seeks designation under the new structure with both

the technical and non-technical path, then about 35% of the mapping work required will be new. Of the 233 combined topics and outcomes in the new mandatory KUs across both paths (technical/non-technical), 42 (18%) are new and 40 (17%) come from previously optional KUs. The old optional KUs (Cybersecurity Planning and Management, Security Program Management, and Security Risk Analysis) included in the new mandatory KUs are no longer available to be chosen as optional.
However, any institution choosing a single path (technical or non-technical) may use any of the required KUs from the non-chosen path as optional KUs.

With the creation of a new non-technical path to CAE designation, there will be some new work for any previously designated CAE to add this track. If a current CAE designated institution seeks designation under the new structure with both the technical and non-technical path, then about 35% of the mapping work required will be new. Of the 233 combined topics and outcomes in the new mandatory KUs across both paths (technical/non-technical), 42 (18%) are new and 40 (17%) come from previously optional KUs. The old optional KUs (Cybersecurity Planning and Management, Security Program Management, and Security Risk Analysis) included in the new mandatory KUs are no longer available to be chosen as optional. However, any institution choosing a single path (technical or non-technical) may use any of the required KUs from the non-chosen path as optional KUs.

5. 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-CD program is a vital part of the process of setting cyber defense curriculum standards and fostering a community of like-minded educational institutions. With a few thousand graduates per year CAE designated schools will probably not eliminate the cybersecurity workforce completely, but will most definitely help with introducing high quality graduates for entry level jobs in the US.

In addition, nationally there are several ongoing high impact programs that address the shortage of cybersecurity professionals, such as National Science Foundation (NSF) grants (capacity building and scholarship for service), regional/national competitions, government-academia-industry partnerships, K-12 outreach programs (e.g. GenCyber), national consortia and collaborations including academia, government, industry, etc. (Chan, et.al. 2017).

We have shared our recent experience applying for CAE-CDE designation in order to inspire and assist others considering doing the same. The analysis of the upcoming changes will assist the higher education institutions seeking designation and scopes the additional work required of schools who will be coming up for re-designation.

6. ACKNOWLEDGEMENTS

We would like to acknowledge our CAE-CD Program mentor, Nelbert (Doc) St. Clair, for his invaluable support during the application process.

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).

Brewer, D., Gilbert, M., Helop, K. (2019). State Of Cybersecurity 2019: Current Trends In Workforce Development. ISACA Report. http://www.isaca.org/Knowledge-Center/Research/Documents/cyber/state-of-cybersecurity-2019-part-1_res_eng_0319.pdf?regnum=505113

Chan, A., El-Sheikh, E., Klappenberger, F., Leary, M., Sande, C., Sands, J., Wesley, D., Zantua, M., Lewis, W. (2017). A Collaborative Response from the NSA/DHS National CAE National Resource Centers (CNRCs) and CAE Regional Resource Centers (CRRCs). https://www.nist.gov/sites/default/files/documents/2017/08/07/national_center_of_academic_excellence_cae_national_resource_centers_cnrcs_and_cae_regional_resource_centers_crrcs.pdf

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

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.

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/

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.

Editor's Note:

This paper was selected for inclusion in the journal as an EDSIGCON 2019 Distinguished Paper. The acceptance rate is typically 7% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2019.

Appendix

Spring 2018 (and earlier)	*Fall 2018 (and beyond)*
Core 2Y KUs	**Foundational CDE KUs**
Basic Data Analysis	Cybersecurity Foundations (CSF)
Basic Scripting	Cybersecurity Principles (CSP)
Cyber Defense	IT Systems Components (ISC)
Cyber Threats	**Core Technical CDE KUs**
Fundamental Security Design Principles	Basic Cryptography (BCY)
Information Assurance Fundamentals	Basic Networking (BNW)
Introduction to Cryptography	Basic Scripting and Programming (BSP)
Information Technology System Components	Network Defense (NDF)
Networking Concepts	Operating Systems Concepts (OSC)
Policy. Legal, Ethics and Compliance	**Core Non-Technical CDE KUs**
Systems Administration	Cyber Threats (CTH)
Core 4Y KUs	Cybersecurity Planning and Management (CPM
Databases	Policy, Legal, Ethics, and Compliance (PLE)
Network Defense	Security Program Management (SPM)
Network Technology and Protocols	Security Risk Analysis (SRA)
Operating Systems Concepts	**Optional KUs (unique to Fall 2018)**
Probability and Statistics	Advanced Algorithms (AAL)
Programming	Basic Cyber Operations (BCO)
Optional KUs (unique to Spring 2018)	Cyber Crime (CCR)
Cybersecurity Planning and Management	Cybersecurity Ethics (CSE)
Overview of Cyber Operations	Databases (DAT)
Security Program Management	Linux System Administration (LSA)
Security Risk Analysis	Network Technology and Protocols (NTP)
	Privacy (PRI)
	Web Application Security (WAS)
	Windows System Administration (WSA)

Optional KUs (common to both)	
Advanced Cryptography (ACR)	Intrusion Detection/Prevention Systems (IDS)
Advanced Network Technology and Protocols (ANT)	Life-Cycle Security (LCS)
Algorithms (ALG)	Low Level Programming (LLP)
Analog Telecommunications (ATC)	Media Forensics (MEF)
Cloud Computing (CCO)	Mobile Technologies (MOT)
Data Administration (DBA)	Network Forensics (NWF)
Data Structures (DST)	Network Security Administration (NSA)
Database Management Systems (DMS)	Operating Systems Hardening (OSH)
Device Forensics (DVF)	Operating Systems Theory (OST)
Digital Communications (DCO)	Penetration Testing (PTT)
Digital Forensics (DFS)	QA/Functional Testing (QAT)
Embedded Systems (EBS)	Radio Frequency Principles (RFP)
Forensic Accounting (FAC)	Secure Programming Practices (SPP)
Formal Methods (FMD)	Software Assurance (SAS)
Fraud Prevention and Management (FPM)	Software Reverse Engineering (SRE)
Hardware Reverse Engineering (HRE)	Software Security Analysis (SSA)
Hardware/Firmware Security (HFS)	Supply Chain Security (SCS)
Host Forensics (HOF)	Systems Certification and Accreditation (SCA)
IA Architectures (IAA)	Systems Programming (SPG)
IA Compliance (IAC)	Systems Security Engineering (SSE)
IA Standards (IAS)	Virtualization Technologies (VTT)
Independent/Directed Study/Research (IDR)	Vulnerability Analysis (VLA)
Industrial Control Systems (ICS)	Wireless Sensor Networks (WSN)
Introduction to Theory of Computation (ITC)	

Table 1 – side-by-side comparison of the required and optional KUs for spring 2018 (and earlier) and fall 2018 (and beyond)

	Fluency in Information Technology	Platform Technologies	Introduction to Computer Science	Professional and Ethical Issues in Computer Science	Management of Database Systems	Business Application Development	Network Fundamentals	Information Security and Assurance	Network System Administration	Ethical Hacking	Introduction to Statistics
Basic Data Analysis											x
Basic Scripting		x	x								
Cyber Defense	x							x	x	x	
Cyber Threats	x							x		x	
Fundamental Security Design Principles							x	x	x	x	
Info Assurance Fundamentals	x							x		x	
Introduction to Cryptography								x		x	
Info Tech System Components	x	x					x	x	x		
Networking Concepts							x	x			
Policy. Legal, Ethics and Compliance	x			x				x		x	
Systems Administration		x					x		x		
Databases	x				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		x			x					
IA Compliance	x			x				x			
IA Standards	x			x				x			
Independent Study										x	
Network Security Administration							x	x	x	x	
Operating Systems Hardening		x							x	x	

Table 2 – mapping of program courses to mandatory and optional KUs for spring 2018

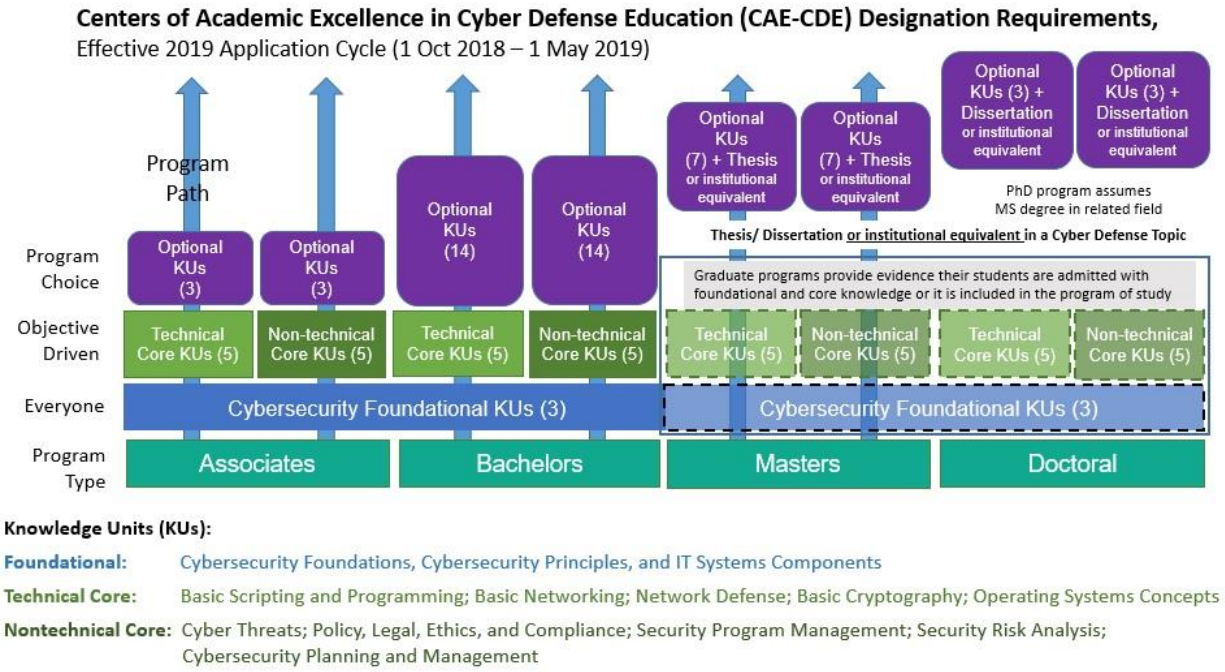

Figure 1 –KU Usage Notional Structure