NATIONAL
CYBERWATCH
CENTER

WHITE PAPERS

ANALYSIS OF THIRD AND FOURTH YEAR UNDERGRADUATE CYBERSECURITY CURRICULUM

AUTHOR: **JIM HOAG, PH.D., CHAMPLAIN COLLEGE, OCTOBER 2017**

Contents

This project is in collaboration with the National CyberWatch Center's National Curriculum Project.

I. Introduction

Cybersecurity is a field that is evolving rapidly and becoming significantly more important in government and industry, as well as technology education. Many colleges have implemented some form of Cybersecurity curriculum. The number, breadth, and depth of courses is expanding to respond to the growth of the field. As the security landscape changes, threat models evolve, and organizations re-factor the role of security. Toward this, course content has changed and been redistributed between courses. The field may be mature enough to standardize elements of the curriculum. This project is designed to identify curriculum components that occur in the third and fourth year of an undergraduate program. One course is analyzed in comparison with the National CyberWatch curriculum, the Centers of Academic Excellence (CAE) Knowledge Units (KUs), and the National Initiative for Cybersecurity Education (NICE) Knowledge, Skills, and Abilities (KSAs).

II.Background

Although Cybersecurity/Information Assurance (IA) is a fairly new academic discipline, there are guidelines for programs and curriculum [1,2,3,4,5] as well as models, effective practices, and suggestions [6,7,8,9,10].

The field of Cybersecurity integrates concepts and skills from a variety of areas including: Computer Science, Cryptography, Information Technology/Systems, Databases, Networks, and Digital Forensics. Cybersecurity programs are emerging from Computer Science, Criminal Justice, Information Technology/Systems, and Business departments. The approach in many cases has been to add security course/content to an existing major. Some institutions have developed academic programs focused on Cybersecurity. Due to the increase in breadth and depth of the field, it has become difficult to offer a comprehensive Cybersecurity experience in an undergraduate program, so schools must determine what areas to focus on.

As the individual academic programs evolve, one goal should be developing a lexicon for Cybersecurity Education. Model degree and certificate programs have been designed for two-year colleges by the National CyberWatch Center [10]. The NSA and DHS have developed guidelines for 2- and 4-year programs as part of the National Centers of Academic Excellence (CAE) in Cybersecurity designation [11].

The primary goal of this project is to investigate third and fourth year undergraduate Cybersecurity courses and to determine if there is a common set of courses that are emerging. Several of these courses or related content are offered in some two-year programs and the third year in four-year programs. This raises the question of whether these courses "belong" in the third year based on the pre-requisite knowledge and courses. Two-year programs are often trying to expose students to elements of security and offer courses/content similar to these. An informal survey of instructors from two-year institutions suggest that if there was additional time (e.g., an additional year at the two-year level), the offering of these courses would be delayed. In addition, this is sometimes an issue when transferring course credits as four-year programs are hesitant to give upper-division credit for 200-level coursework.

A secondary goal of this project is to analyze the course content and learning objectives of courses offered in both 2- and 4-year institutions to determine if there are differences in the pre-requisite knowledge and complexity level of learning objectives. This may lead to a distinction between the 2- and 4-year version of these courses and aid in articulation agreements.

A third goal of this project to analyze the course content in association with the NICE Framework KSA's. Some preliminary work has been done in this area as part of the National CyberWatch Center's National Curriculum Committee [13]

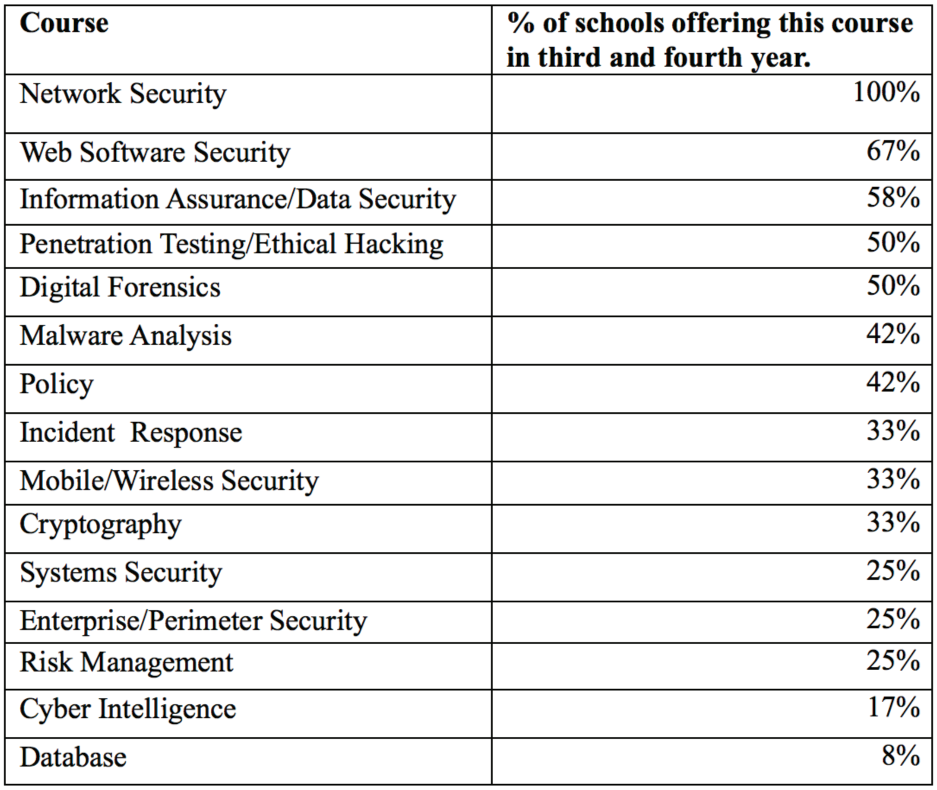
III. Investigation

Third and fourth year Cybersecurity courses from twelve colleges have been analyzed for title, course description, and learning objectives (when available) to try to find common courses or topics taught. Schools were selected from those designated as Centers of Academic Excellence in Information Assurance/Cyber Defense (CAE/IA-CD) [11four-year programs. As of October 2017, there are approximately 230 CAE/IA-CD, of which approximately 140 are 4-year programs in Cyber Defense. The curriculum of some of these institutions were analyzed as part of two earlier studies [13][14]

The institutions included :

- California Polytechnic University, Pomona
- Capitol Technical University
- Champlain College
- Dakota State University
- Eastern Michigan University
- Ferris State University
- Kennesaw State University
- Mercy College
- Rochester Institute of Technology
- Towson University
- Tuskegee University
- Wilmington University

The 300-400 level courses were grouped by course title, description, and when available, topics and learning objectives. The titles of the courses differed and sometimes covered multiple topics. The following fifteen courses or course content areas emerged. The percent of programs offering the courses was calculated and is presented in Table 1.



Course	% of schools offering this course in third and fourth year.
Network Security	100%
Web Software Security	67%
Information Assurance/Data Security	58%
Penetration Testing/Ethical Hacking	50%
Digital Forensics	50%
Malware Analysis	42%
Policy	42%
Incident Response	33%
Mobile/Wireless Security	33%
Cryptography	33%
Systems Security	25%
Enterprise/Perimeter Security	25%
Risk Management	25%
Cyber Intelligence	17%
Database	8%

Table 1 : Common 3rd-4th year Cybersecurity courses. Raw data available upon request.

Since the Network Security course was common to all schools, it was used as a prototype case, and was analyzed and compared with the model courses from National CyberWatch and two-year curriculum, the CAE Knowledge Units, and the NICE Workforce Framework KSAs. The courses had descriptions and topics similar to the CAE Network Defense KU so those topics were used in comparisons. It might seem more appropriate to use the learning objectives, but it was found that the learning objectives from the CAE Network Defense KU were at the same time too broadly worded and simplistic:

- Students will be able to describe the various concepts in network defense
- Students will be able to apply their knowledge to implement network defense measures.
- Students will be able to use network monitoring tools (e.g., WireShark).
- Students will be able to use a network mapping tool (e.g., Nmap).

Note the first two learning objectives are quite broad. The last two do not reflect a level of maturity that matched the third year courses. In fact, these two objectives are identical to those required in the 2-year CAE Core Network Concepts KU. Thus, the list of topics was used as it more closely matched the content of the college courses sampled.

Comparision of 3rd Year Course with CyberWatch's 2 Year Curriculum

The topics in the CAE Network Defense KU were compared with topics covered in the second year National CyberWatch curriculum. Again, the learning objectives for the CAE Network Defense KU are too broad to use in comparison with learning objectives for the National CyberWatch course.

Two National CyberWatch courses appear to have a subset of the topics in the CAE Network Defense KU: NCC 213: IDS/IPS Fundamentals and NCC 220: Network Security:

CAE Knowledge Unit Topics	**CyberWatch Course Topics**	
Network Defense	**NCC 213 IDS IPS**	**NCC 220 Network Security**
1. Implementing IDS/IPS	1.0 Network- and Host-Based IDS/IPS Solutions	
2. Implementing Firewalls, VPNs		4.0 Implementing Firewall Technologies 7.0 Implementing VPNs
3. Defense in Depth		
4. Honeypots and Honeynets		
5. Network Monitoring	4.0 Filters/Rules for Net Monitoring 5.0 Intro to Net Security Monitoring	
6. Network Traffic Analysis	2.0 Fund. of Traffic Analysis 3.0 Advanced Traffic Analysis	
7. Minimizing Exposure (Attack Surface and Vectors)		
8. Network Access Control (internal and external)		3.0 Authentication, Authorization, and Accounting
9. DMZs / Proxy Servers		
10. Network Hardening		2.0 Securing Network Devices 5.0 Securing LAN 8.0 Managing a Secure Network
11. Mission Assurance		
12. Network Policy Dev/ Enforcement		
13. Network Operational Procedures		
14. Network Attacks		1.0 Modern Net Security Threats
	6.0 Analyzing/ Deconstructing Attack Signatures	6.0 Cryptographic Systems

Table 2: Comparison of Topics in CAE Network Security KU and National CyberWatch curriculum

Note that CAE Network Defense topics 3,4,7,9.11,12,13 do not match content in the 2-year National CyberWatch courses. The topics may in fact be covered within those courses, but it is not evident from the information available. The CAE Network Defense KUs geared toward third and fourth year programs contains topics that would not be included in the National CyberWatch curriculum. In addition, some topics appear more complex in nature and would build on the topics in the National CyberWatch courses. Notably, the topics of Defense-in-Depth, Mission Assurance, and Policy Development seem to be content areas covered in the third and fourth year courses. Technical topics such as DMZ/Proxy Servers and Honeypots/Nets are also focus areas in this KU and might be covered in the courses, but are not specified.

Comparison with NSA/DHS Knowledge Units

The common courses listed in Table 1 can be associated with the KUs used as a criteria for 4-year CAE institutions as shown in Table 3:

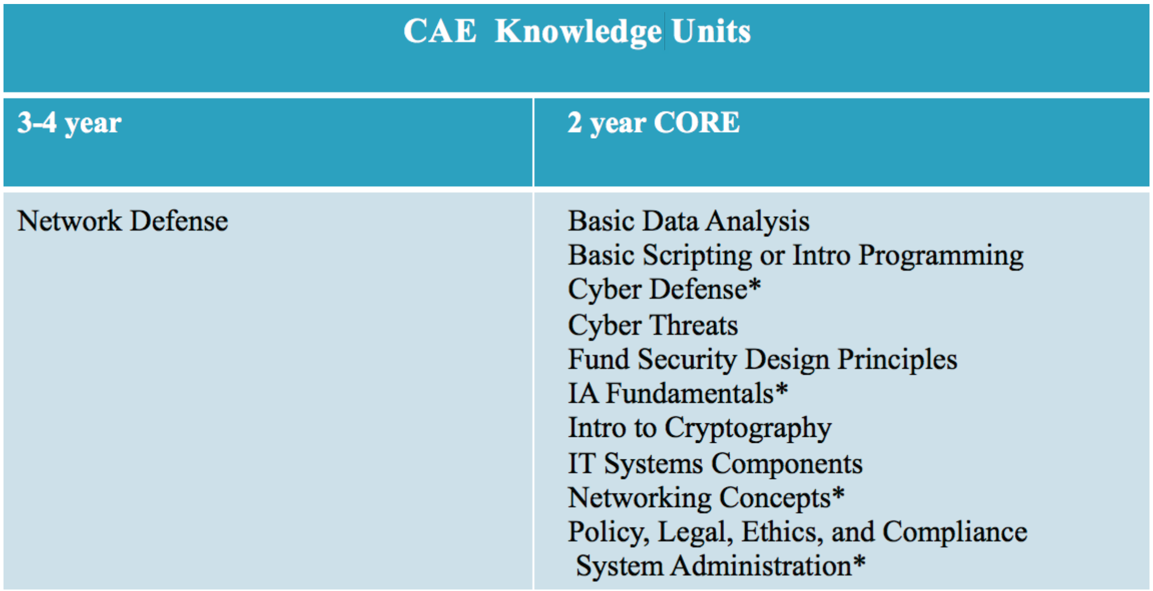
Common Courses from CAE 4 year programs	**4 year CAE - Knowledge Units** **Black -> required, Green -> Optional**
Network Security	Net Defense, Net Tech & Protocols, Network Security Administration, Intrusion Detection
Web/Software Security	Secure Programming Practices
Information Assurance/Data Security	IA Standards/Compliance
Penetration Testing/Ethical Hacking	Penetration Testing
Digital Forensics	Digital Forensics

Table 3 : CAE KUs and Common Third and Fourth year security courses

Network Security is a course offered by all the CAE's analyzed. The closest associated KU for 4-year programs is Network Defense and is also one of the CAE KUs for 4-year schools. This KU will be used as a prototype for analyzing third and fourth year CAE Cybersecurity courses in association with CAE first and second year courses.

While the CAE KU's are delineated between 2-year and 4-year curriculum, there is no hierarchy in the courses or prerequisite structure. It might be interesting and useful to establish a pathway through the KU's.

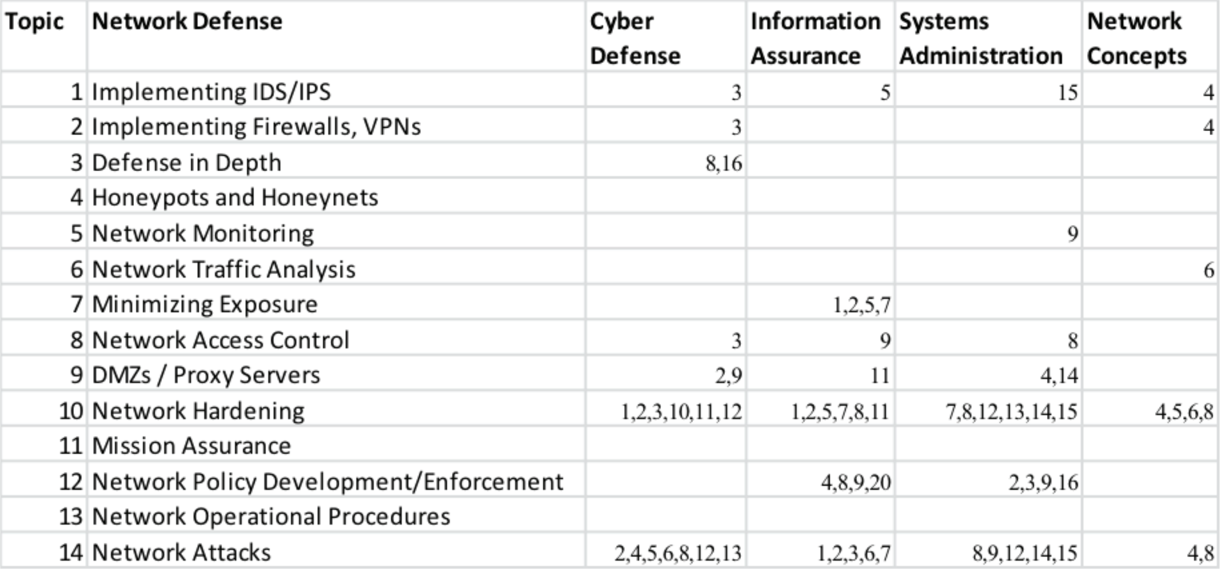
In Table 4. the 2-year CAE Core KUs are listed to associate pre-requisite knowledge with the course. Four KUs were selected as pre-requisite knowledge based on the course description, topics covered, and learning objectives. These are indicated in asterisks in the following table:



CAE Knowledge Units	
3-4 year	**2 year CORE**
Network Defense	Basic Data Analysis Basic Scripting or Intro Programming Cyber Defense* Cyber Threats Fund Security Design Principles IA Fundamentals* Intro to Cryptography IT Systems Components Networking Concepts* Policy, Legal, Ethics, and Compliance System Administration*

Table 4. Potential Pre-requisite KUs for Network Defense KU noted with *

The courses were compared in terms of the course description, topics, and learning objectives in Table 3 to determine a possible set of pre-requisite courses. Appendix I includes a comparison of course descriptions, learning objectives, and course topics for Network Defense and the four courses with pre-requisite knowledge. The goal is to determine which topics are unique to the third year course indicating a higher level of understanding/comprehension. Table 5 below contains mappings of pre-requisite topics from the 4 classes for topics in Network Defense:



Topic	Network Defense	Cyber Defense	Information Assurance	Systems Administration	Network Concepts
1	Implementing IDS/IPS	3	5	15	4
2	Implementing Firewalls, VPNs	3			4
3	Defense in Depth	8,16			
4	Honeypots and Honeynets				
5	Network Monitoring			9	
6	Network Traffic Analysis				6
7	Minimizing Exposure		1,2,5,7		
8	Network Access Control	3	9	8	
9	DMZs / Proxy Servers	2,9	11	4,14	
10	Network Hardening	1,2,3,10,11,12	1,2,5,7,8,11	7,8,12,13,14,15	4,5,6,8
11	Mission Assurance				
12	Network Policy Development/Enforcement		4,8,9,20	2,3,9,16	
13	Network Operational Procedures				
14	Network Attacks	2,4,5,6,8,12,13	1,2,3,6,7	8,9,12,14,15	4,8

Table 5. Mapping of similar topics between Network Defense KU and 2-year Core KUs

The mapping indicates some topics are heavily covered in 2-year courses while others are not. We could assume then that the 2-year courses provide pre-requisite background for some topics that are covered in the Network Defense KU and that other topics are new or build on the pre-requisite knowledge.

Topics that appear to be added in the Network Defense course include Defense-in-Depth, Honeypots/Nets, Network Monitoring, Traffic Analysis, Minimizing Exposure, Mission Assurance, and Network Operational Procedures. Network Monitoring and Traffic Analysis are covered in the 2-year KUs. Likewise, some of the other topics might be mentioned in the 2-year KUs. The difference should be in the depth of the topic. The learning objective in a 2-year KU might be understanding the concept of Defense-in-Depth, while the third and fourth year curriculum would include design, implementation, and maintenance. The nature of these topics would indicate that the content has design, planning, integration, and strategic goals as well as implementation of network defense technology(ies). This is associated with higher-level learning/thinking than the 2-year courses as we would hope for. This corresponds to the comparison with the National CyberWatch curriculum.

While the learning objectives for Network Defense seemed inadequate for analysis, we can do some comparison. The primary learning objective for Network Defense suggest that students will apply their knowledge to implement network defense measures. The learning objectives for the 2-year courses have learning objectives based on phrasing such as describe, examine, install, and use. However, there are similar learning objectives in the Cyber Defense KU: apply cyber defense methods to prepare a system to repel attacks, and the learning objective in Information Assurance: examine the architecture of a typical, complex system and identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be employed.

The third and fourth learning objectives for the Network Defense KU are identical to those for the CAE 2-year Network Concepts Core KU. Based on this analysis, those should be revised to reflect a higher level of reasoning: i.e. use network monitoring and mapping tools to analyze network traffic, performance, and security issues.

Analysis Using KSA's

Another method used to compare the 1-2 pre-requisite courses and the third and fourth year Network Defense class is to analyze them in terms of smaller composite elements (NICE KSA's) and attempt to characterize the differences between the courses. There have been several efforts to map curriculum to the NICE KSA's [13,15]. One such project in 2014 involved asking Subject Matter Experts (SME) to establish correspondence between the NSA/DHS KUs and the NICE KSA's [15]. Using these mappings of CAE KUs to NICE KSAs, the NICE KSA's associated with the first and second year KU's were analyzed in relation to the KSA's associated with the Network Defense KU.

The assumption was that the first and second year KU's would provide a foundation for additional learning in the third and fourth year course. Using KSAs to characterize the course content indicates no additional content covered in the Network Defense KU. The KSA's were compared using Excel functions and the data was also analyzed by creating Venn Diagrams from the KSA for each course. This provides the clearer interpretation.

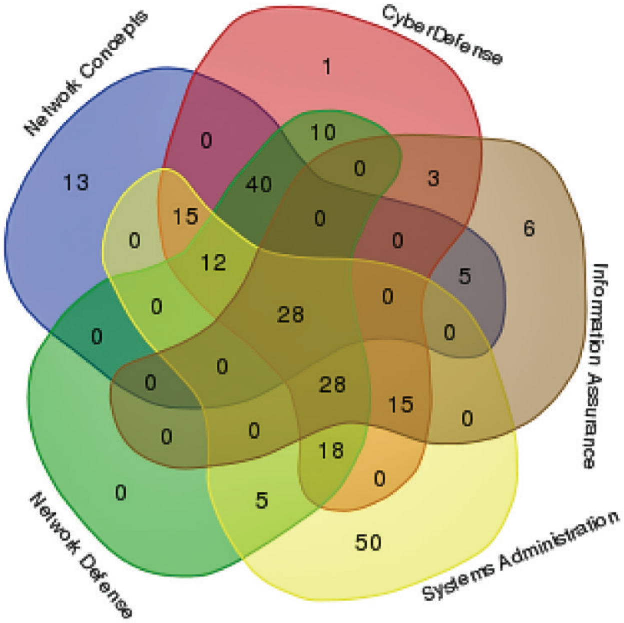


Figure 1. Venn Diagram of KSA content of KUs (created with tool provided at http://bioinformatics.psb.ugent.be/cgi-bin/liste/Venn/calculate_venn.htpl)

Surprisingly, using this analysis technique, there are no KSA's unique to the Network Defense (ND) KU when compared to the Network Concepts (NC) KU, Cyber Defense (CD), Information Assurance (IA), and Systems Administration (SA) KUs. This implies that all pertinent knowledge was covered in the first and second year KUs. Also, based on this analysis, several KUs contribute little additional knowledge: Cyber Defense - 1 additional KSA, and Information Assurance - 6 additional KSAs.

In addition, this analysis would suggest re-alignment of the first and second year content. 28 KSAs are common to all 5 KUs. This might represent a common body of knowledge that might be taught prior to all or comprise a fundamental KU. Another 40 KSAs are shared between NC, CD, ND and 28 more between CD, ND, IA, SA. These might represent a fundamental set of concepts, which if combined with the 28 KSAs common to all could be used as pre-requisite knowledge for all of these KUs. Examination of the 28 common KSA gives a different perspective. These are not fundamental concepts. This analysis also does not correspond to the findings of the other comparison where elements like Defense in Depth are unique to the KU:

1. Knowledge of and experience in Insider Threat investigations, reporting, investigative tools and laws/regulations.
2. Knowledge of virtual machine aware malware, debugger aware malware, and packing.
3. Knowledge of cyber defense policies, procedures, and regulations.
4. Skill in protecting a network against malware.
5. Knowledge of intrusion detection methodologies and techniques for detecting host-and network-based intrusions via intrusion detection technologies.
6. Knowledge of defense-in-depth principles and network security architecture.
7. Knowledge of malware analysis concepts and methodology.
8. Skill in mimicking threat behaviors.
9. Knowledge of common attack vectors on the network layer.
10. Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored]).
11. Skill in analyzing anomalous code as malicious or benign.
12. Skill in deep analysis of captured malicious code (e.g., malware forensics).
13. Ability to apply supply chain risk management standards.
14. Knowledge of the types of Intrusion Detection System (IDS) hardware and software.
15. Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution).
16. Skill in tuning sensors.
17. Knowledge of cyber defense mitigation techniques and vulnerability assessment tools, including open source tools, and their capabilities.
18. Knowledge of Intrusion Detection System (IDS) tools and applications.
19. Skill in identifying obfuscation techniques.
20. Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).
21. Skill of identifying capturing, containing, and reporting malware.
22. Skill in collecting data from a variety of cyber defense resources.
23. Knowledge of content development.
24. Knowledge of general attack stages (e.g., foot printing and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks).
25. Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).
26. Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures (TTP).
27. Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning

for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).

28. Knowledge of common adversary tactics, techniques, and procedures (TTPs) in assigned area of responsibility (e.g., historical country-specific TTPs, emerging capabilities).

This suggests that the mappings of KUs to KSAs may have some inaccuracies or that the current version of KSAs do not translate well into curricula. However, it may also be that the KSAs and KUs were designed for different purposes/groups and developing relevant mappings with the current versions will be difficult. KUs may someday map to a subset of the KSAs to indicate what KSA should be included in a Cybersecurity academic program. The pre-requisite structure is a critical component of curriculum and that is not yet part of either the KSA Framework or the KUs.

Conclusion

The research question was: what should third and fourth year Cybersecurity courses cover, given the content of many 2-year programs? An analysis based on topics, the NSA/DHS KUs, and the National CyberWatch Network Security course, offered at all 4-year CAE institutions sampled, indicates that some of the topics are appropriate for learning beyond the pre-requisite two-year content. A further analysis of the content of this course and several others: Web/Software Security, Information Assurance/Data Security, Penetration Testing/Ethical Hacking might help establish standards for third and fourth year curriculum. Comparing these findings to the new version of the Association of Computing Machinery (ACM)/Institute for Electrical and Electronics (IEE) curriculum guidelines would be useful as well. Analysis using the NICE KSAs indicates there may be some KSAs that are common to multiple KUs and might be able to be used as foundational knowledge structure.

References

[1]Cooper, S., Nickell, C., Piotrowski, V., Oldfield. B., Abdallah., A., Bishop, M. , Caelli, B. , Dark, M. , Hawthorne, E. K., Hoffman, L. , Pérez, L. , Pfleeger. C. , Richard Raines, R. , Schou. C. 2009 , Toward a Framework for Information Assurance Education, ITiCSE_2009

[2] Cooper, S. , Nickell, C., Pérez, L. , Oldfield, B., Brynielsson, J. , Gencer Gökce, A. , Hawthorne, E. K. , Klee, K. J. , Andrea Lawrence, A. , Wetzel, S. 2010, Towards Information assurance (IA) curricular guidelines, Proceedings of the 2010 ITiCSE working group reports, June 28-30, Ankara, Turkey

[3] Manson, D., Curl, S., Torner, J. 2009, A Framework for Improving Information Assurance Education, Communications of the IIMA. 79. Volume 9, Issue 1.

[4] McGettrick, A., Cassel, L.N., Dark, M, .Hawthorne, E.K., Impagliazzo, J. 2014, Toward Curricular Guidelines for Cybersecurity. SIGCSE'14 Atlanta, Ga

[5] ACM Computer Science Curriculum 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science (Dec. 2013); doi: 10.1145/2534860

[6] Conti, G. , Hill, J , Lathrop, S. , Alford, K., Ragsdale, D. 2003, A comprehensive undergraduate information assurance program, Security education and critical infrastructures, Kluwer Academic Publishers, Norwell, MA,

[7] Smith, T., Koohang, A., Behling, R. 2010, Formulating an Effective Cybersecurity Curriculum, International Association for Computer Information Systems

[8] Hoag, J. 2013 Evolution of Cybersecurity Curriculum, InfosecCD 13

[9] Whitman, M. E., Mattord, H.J. 2004, A Draft Model Curriculum for Programs of Study in Information Security and Assurance, Proceedings of the 8th Collquium for Information Systems Security, West Point, NY June.

[10] CyberWatch: http://www.nationalcyberwatch.org/programs-resources/curriculum/

[11] http://www.nsa.gov/ia/academic_outreach/nat_cae/

[12] National Cybersecurity Workforce Framework. http://csrc.nist.gov/nice/framework/

[13] National CyberWatch Center: Collaborative Curriculum Taskforce https://atecentral.net/r31138/collaborative_curriculum_taskforce_study_of_the_cybersecurity_workforce_framework_mapping_to_academic_courses

[14] Hoag, J., 2015, An Analysis of Academic Background Factors and Performance in Cyber Defense Competitions, International Security Education Journal (ISEJ), 2015

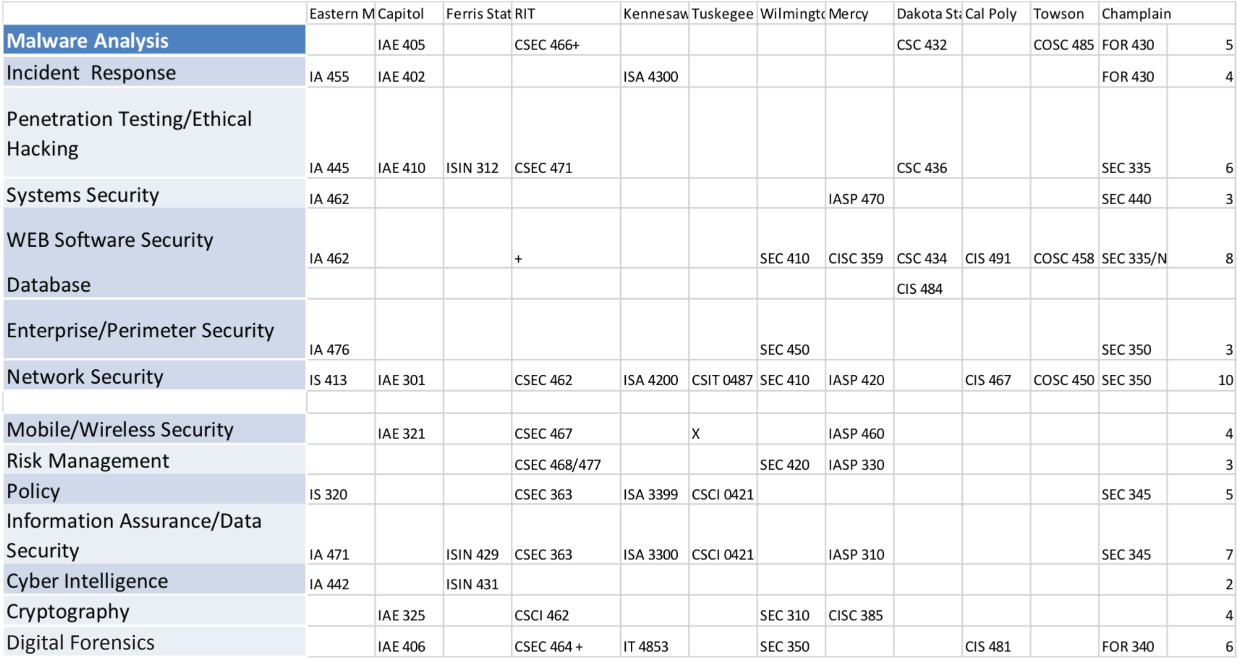
[15] Mapping NSA/DHS Knowledge Units to NICE Framework 2.0 https://niccs.us-cert.gov/sites/default/files/documents/pdf/mapping_nsa_dhs_knowledge_unit_to_nice_fw_2.0.pdf?trackDocs=mapping_nsa_dhs_knowledge_unit_to_nice_fw_2.0.pdf

Appendix

1. Chart of schools and courses
2. Comparison of Network Defense Knowledge Unit and pre-req courses
    a. Descriptions
    b. Learning Objectives
    c. Topics
3. Excel summary results for comparison of SME-KU-KSA mappings

Appendix I

Chart of Schools and Courses

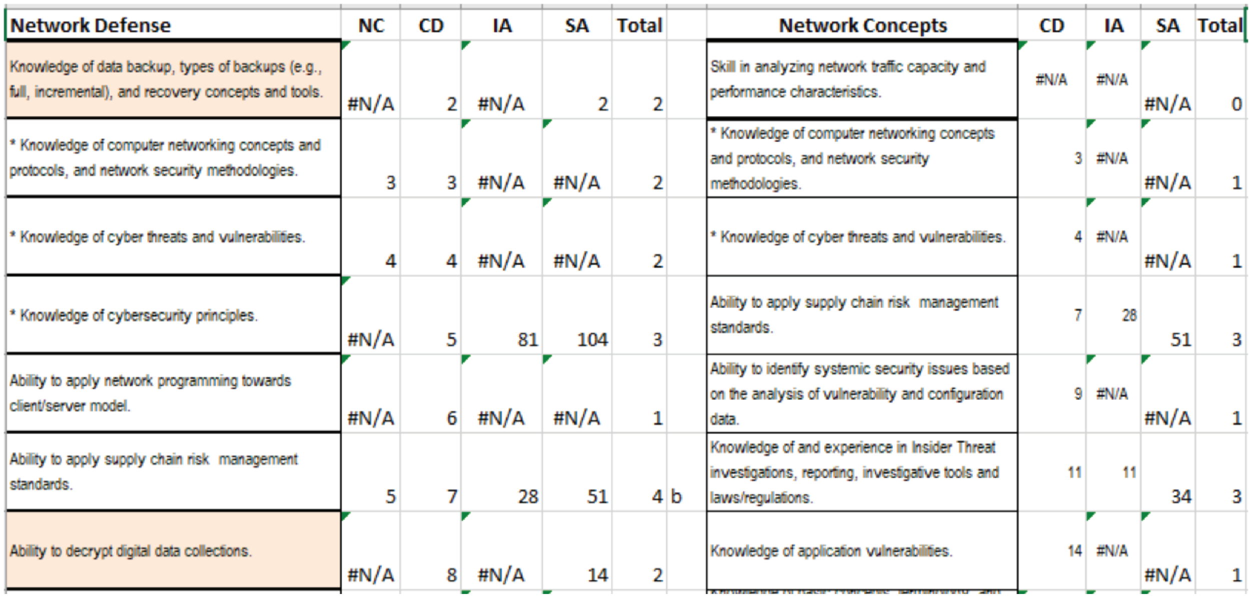


	Eastern M	Capitol	Ferris Stat	RIT	Kennesaw	Tuskegee	Wilmingtc	Mercy	Dakota Stε	Cal Poly	Towson	Champlain	
Malware Analysis		IAE 405		CSEC 466+					CSC 432		COSC 485	FOR 430	5
Incident Response	IA 455	IAE 402			ISA 4300							FOR 430	4
Penetration Testing/Ethical Hacking	IA 445	IAE 410	ISIN 312	CSEC 471					CSC 436			SEC 335	6
Systems Security	IA 462							IASP 470				SEC 440	3
WEB Software Security	IA 462			+			SEC 410	CISC 359	CSC 434	CIS 491	COSC 458	SEC 335/N	8
Database									CIS 484				
Enterprise/Perimeter Security	IA 476						SEC 450					SEC 350	3
Network Security	IS 413	IAE 301		CSEC 462	ISA 4200	CSIT 0487	SEC 410	IASP 420		CIS 467	COSC 450	SEC 350	10
Mobile/Wireless Security		IAE 321		CSEC 467		X		IASP 460					4
Risk Management				CSEC 468/477			SEC 420	IASP 330					3
Policy	IS 320			CSEC 363	ISA 3399	CSCI 0421						SEC 345	5
Information Assurance/Data Security	IA 471		ISIN 429	CSEC 363	ISA 3300	CSCI 0421		IASP 310				SEC 345	7
Cyber Intelligence	IA 442		ISIN 431										2
Cryptography		IAE 325		CSCI 462			SEC 310	CISC 385					4
Digital Forensics		IAE 406		CSEC 464 +	IT 4853		SEC 350			CIS 481		FOR 340	6

Appendix II

Comparison of Network Defense Knowledge Unit and Pre-req Courses

A sample of one technique used to compare the KSA's associated with Network Defense with the KSA's of KU's that might be pre-requisite. The KSA's for each KU (Network Defense, Network Concepts, Cyber Defense, Systems Administration, and Information Assurance) were compared using a match() function. In this sample, only the KSA's for Network Defense and Network Concepts are shown along with matches from the other KU's The actual data set is larger and can be obtained by contacting the author.



Network Defense	NC	CD	IA	SA	Total		Network Concepts	CD	IA	SA	Total
Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools.	#N/A	2	#N/A	2	2		Skill in analyzing network traffic capacity and performance characteristics.	#N/A	#N/A	#N/A	0
* Knowledge of computer networking concepts and protocols, and network security methodologies.	3	3	#N/A	#N/A	2		* Knowledge of computer networking concepts and protocols, and network security methodologies.	3	#N/A	#N/A	1
* Knowledge of cyber threats and vulnerabilities.	4	4	#N/A	#N/A	2		* Knowledge of cyber threats and vulnerabilities.	4	#N/A	#N/A	1
* Knowledge of cybersecurity principles.	#N/A	5	81	104	3		Ability to apply supply chain risk management standards.	7	28	51	3
Ability to apply network programming towards client/server model.	#N/A	6	#N/A	#N/A	1		Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.	9	#N/A	#N/A	1
Ability to apply supply chain risk management standards.	5	7	28	51	4	b	Knowledge of and experience in Insider Threat investigations, reporting, investigative tools and laws/regulations.	11	11	34	3
Ability to decrypt digital data collections.	#N/A	8	#N/A	14	2		Knowledge of application vulnerabilities.	14	#N/A	#N/A	1

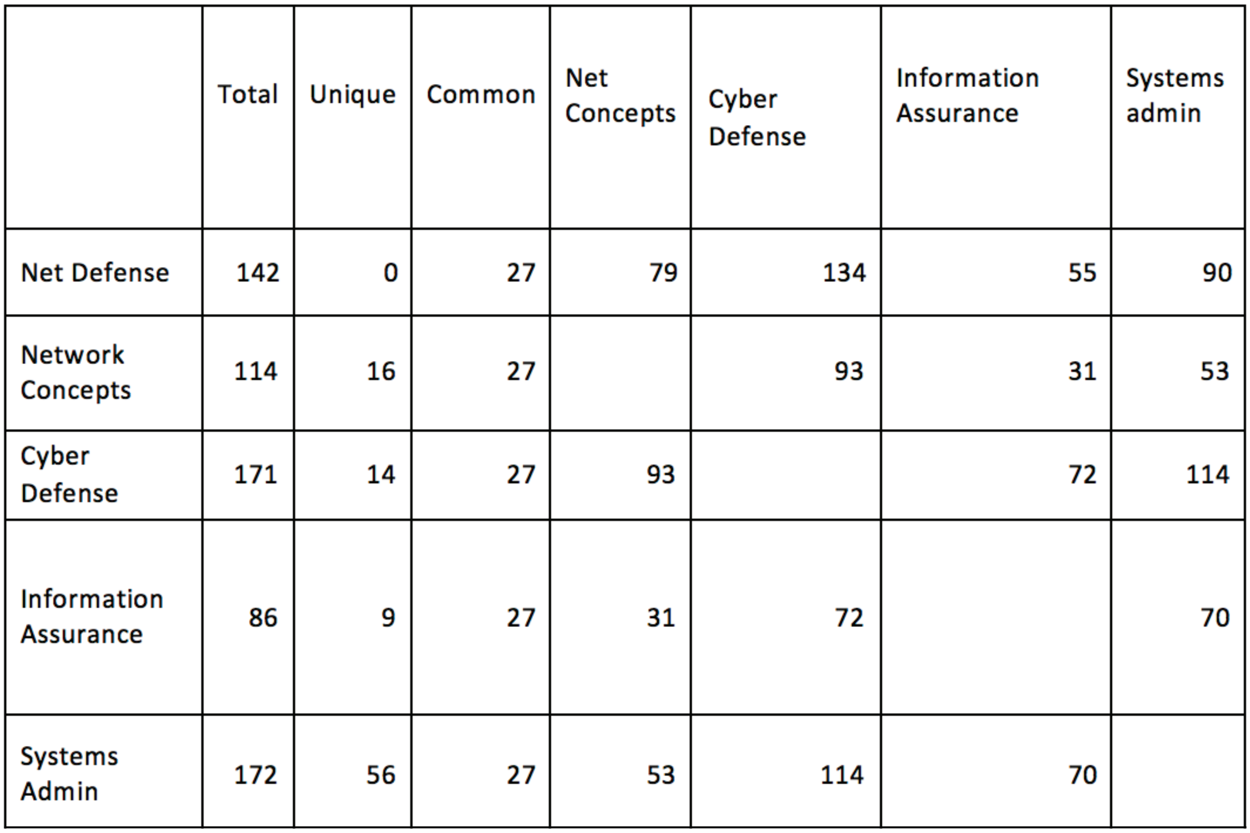
Appendix III

Summary of KU KSA overlap , unique KSAs using Excel.

Values are close to those obtained using Venn Diagram tool.

27 common KSAs vs 28 in the Venn Diagram

93 KSA's common between Network Concepts and Cyber Defense vs 95 in the Venn Diagram.



	Total	Unique	Common	Net Concepts	Cyber Defense	Information Assurance	Systems admin
Net Defense	142	0	27	79	134	55	90
Network Concepts	114	16	27		93	31	53
Cyber Defense	171	14	27	93		72	114
Information Assurance	86	9	27	31	72		70
Systems Admin	172	56	27	53	114	70	

NATIONAL
CYBERWATCH
CENTER

CYBERSECURITY EDUCATION
SOLUTIONS FOR THE NATION

National CyberWatch Center
Prince George's Community College
Room 129B
301 Largo Road
Largo, MD 20774

www.nationalcyberwatch.org