Developing a Cybersecurity Curriculum and Assessment using the New ABET Student Outcomes

Judson Dressler
judson.dressler@usafa.edu

Bobby Birrer
bobby.birrer@usafa.edu

Lucille McMinn
lucille.mcminn@gmail.com

Matthew Sievers
matt.d.sievers@gmail.com

David Caswell
david.caswell@usafa.edu

Department of Computer and
Cyber Sciences
United States Air Force Academy
Colorado Springs, CO USA

Abstract - With the recent updates to ABET's Criteria for Accrediting Computing Programs as well as the addition of the new cybersecurity program, opportunities for innovation and efficiencies have emerged. As we continue to build-out our Cyber Science program, exploring these new opportunities resulted in a streamlined management and assessment process while providing great opportunity to create and maintain a robust and relevant program. This paper documents the recent ABET changes and describes how one of the first ABET accredited cybersecurity programs is meeting these new standards.

Keywords
Cyber, Security, Curriculum Design, Assessment, Accreditation, ABET, Student Outcomes

1. INTRODUCTION

The United States Air Force Academy (USAFA) has offered a cybersecurity degree since 2014. The recent addition of ABET's cybersecurity program precipitated and enabled a relook at how our Department of Computer and Cyber Sciences define, develop, and assess accomplishment of our Cyber Science program goals. Additionally, the new streamlined Computing Accreditation Commission (CAC) Student Outcomes became more targeted and statistically independent. The new Student Outcomes also align more closely with our Higher Learning Commission-based institutional outcomes allowing development and assessment of our department's program-based Student Outcomes to serve dual-purpose contributing more directly to the accomplishment of the institutional outcomes. This simplified the mapping of program Student Outcomes to institutional outcomes enabling more effective accomplishment of both while easing the assessment workload.

This paper summarizes the latest two updates to the ABET CAC Criteria for Accrediting Computing Programs, describes how the new Student Outcomes map to and complement our institutional outcomes and National Security Agency Center of Academic Excellence in Cyber Operations criteria, and then elaborates how our Cyber Science program Student Outcomes are developed and assessed in a cross-curricular program design. This dialog includes specific examples of how courses contribute to the accomplishment of new Student Outcomes.

2. BACKGROUND

USAFA established a Bachelor of Science program in cyber security in 2014 under the title Computer Network Security. Offered by the Department of Computer Science, students first graduated from the program in 2016. Without ABET criteria available at the time, this major was primarily designed to satisfy the National Security Agency's (NSA) Center of Academic Excellence in Cyber Operations (CAE-CO), which was awarded to USAFA in 2016. A comparison of the newly established ABET student outcomes to the NSA CAE-CO requirements is discussed in Section 2.

In 2016, both IEEE and CSAB established committees to create ABET criteria for cybersecurity computing programs [1]. Previously, any cybersecurity programs seeking accreditation were required to meet the CAC General Criteria. The Computing Area Delegation approved the results of both committees in August of 2017 and released them for public review and comment until June 2018. ABET formally approved the program-specific criteria for cybersecurity in 2017 [1]. The United States Air Force Academy, United States Naval Academy, Towson University, and Southeast Missouri State University participated in a pilot program to receive accreditation under the proposed criteria and student outcomes while still under development [2]. The student outcomes under the proposed criteria replaced general outcomes for communication, analyzing impacts, professional development, and using current techniques and tools with new outcomes pertaining to applying security principles and practice and analyzing and evaluating systems with respect to maintaining operations in the presence of risks and threats. USAFA and the other three institutions each received accreditation under the proposed criteria in November 2018 [2]. The finalized criteria and student outcomes reintroduced communications as a student outcome, consolidated problem analysis and application of knowledge into a single outcome, and combined the two cybersecurity program-specific outcomes in a single outcome. The progression of the student outcomes from the CAC general student outcomes to the proposed cybersecurity student outcomes to the finalized student outcomes is shown in Table 1.

Table 1: Evolution of the ABET Cybersecurity Student Outcomes

Previous Computing Accreditation Commission General Student Outcomes [3]	**Proposed 2018-2019 Cybersecurity Student Outcomes** [4]	**Current 2019-2020 Cybersecurity Student Outcomes** [5]
An ability to apply knowledge of computing and mathematics appropriate to program's student outcomes and the discipline	An ability to apply knowledge of computing and mathematics appropriate to the program's student outcomes and to the discipline	Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution	An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution	Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in context of program's discipline.
An ability to design, implement, and evaluate a computer-based system, process, component, or program to meet needs	An ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs	Communicate effectively in a variety of professional contexts.
An ability to function effectively on teams to accomplish a common goal	An ability to function effectively on teams to accomplish a common goal	Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.
An understanding of professional, ethical, legal, security and social issues and responsibilities	An understanding of professional, ethical, legal, security and social issues and responsibilities	Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.
An ability to communicate effectively with a range of audiences	An ability to apply security principles and practices to the environment, hardware, software, and human aspects of a system. [Cybersecurity Program-Specific]	Apply security principles and practices to maintain operations in the presence of risks and threats. [Cybersecurity Program-Specific]
An ability to analyze the local and global impact of computing on individuals, organizations, and society	An ability to analyze and evaluate systems with respect to maintaining operations in the presence of risks and threats. [Cybersecurity Program-Specific]	
Recognition of the need for and an ability to engage in continuing professional development		
An ability to use current techniques, skills, and tools necessary for computing practice.		

At the USAFA institutional level, nine outcomes, established based upon Higher Learning Commission guidance, provide direction for the core curriculum, all academic major programs, physical education, leadership, and military education and training programs. These nine institutional outcomes address Critical Thinking; Clear Communications; Application of Engineering Methods; Scientific Reasoning and the Principles of Science; the Human Condition, Cultures, and Societies; Leadership, Teamwork and Organizational Management; Ethics and Respect for Human Dignity; National Security of the American Republic; and Warrior Ethos as Airmen and Citizens [6]. All academic major programs must help to develop and assess the critical thinking and clear communications outcomes. Additionally, two of the required courses for the Cyber Science major also formally address the Application of Engineering Methods outcome. While not mandated, the Cyber Science program informally addresses each of the remaining six institutional outcomes. Comparing our Cyber Science Student Outcomes (CS-SOs) with the institutional outcomes, we find natural overlaps that include:

- CS-SOs 1, 2 with Application of Engineering Methods, Scientific Reasoning and the Principles of Science
- CS-SO 3 with Clear Communications
- CS-SO 4 with Critical Thinking, Ethics and Respect for Human Dignity, the Human Condition, Cultures, and Societies
- CS-SO 5 with Leadership, Teamwork, and Organizational Management
- CS-SO 6 with National Security of the American Republic, Warrior Ethos as Airmen and Citizens

USAFA is also designated under the National Security Agency's National Centers of Academic Excellence in Cyber Operations Program. USAFA maps courses to both ABET's 2019-2020 standard for Cybersecurity student outcomes and the CAE-CO program's requirements. The ABET criteria and the NSA CAE-CO criteria have synergies satisfying both programs with many of the same courses. Overall, ABET provides self-determination for program content whereas CAE-CO imposes more specific technical requirements with some choice among the optional content. Notable differences between NSA CAE-CO and ABET's requirements include:

1) Mandatory and optional content as opposed to ABET's student outcomes with high-level prescribed content,

2) Interdisciplinary integration of cyber operations beyond technical specialization (i.e. social and legal content) which goes a step further than ABET's ethics inclusion and impacts of computing requirement,

3) Students required participation in cyber-operations related research as opposed to ABET's focus on faculty research and institutional involvement.

Currently 14 programs at 12 institutions are CAE-CO designated at the Bachelor of Science level whereas ABET lists 4 accredited Cybersecurity programs at 4 institutions at the same level (ABET, 2019) (NSA, 2019). A brief overview of the CAE-CO knowledge units follows in Table 2. The CAE-CO mandatory and optional knowledge units are cross-mapped primarily to ABET's Outcomes 1, 2, 4, and 6 and address the required ABET Program Criteria topics. Highlighted are USAFA's specific selection of optional knowledge units.

USAFA's status as a military academy drives a focus of optional knowledge toward hands-on offensive cyber operations and practical vulnerability research-related topics rather than information technology (virtualization, cloud, systems and software development) topics.

Other influences that guide our Cyber Science program include an extensive core curriculum that limits majors courses to sixteen including electives, curricular guidance such as the Computer Science Curricula 2013 [7] and the Cybersecurity Curricula 2017 [8] documents, and the requirements of other academic programs which utilize some of the same courses in in our Cyber Science program.

Table 2 - NSA CAE-CO Requirements with USAFA Optional Selections Highlighted

Mandatory Knowledge Units	Optional Knowledge Units (10 of 17 required)
1. Low-level programming (C and assembly) 2. Software Reverse Engineering 3. Operating System Theory 4. Networking 5. Cellular and Mobile Technologies 6. Discrete Math and Algorithms 7. Overview of Cyber Defense 8. Security Fundamental Principles 9. Vulnerabilities 10. Legal and Ethics	**1. Programmable Logic** **2. Wireless Security** 3. Virtualization 4. Cloud Security/Cloud Computing **5. Risk Management of Information Systems** **6. Computer Architecture** 7. Microcontroller Design **8. Software Security Analysis** 9. Secure Software Development **10. Embedded Systems** **11. Digital Forensics** 12. Systems Programming **13. Applied Cryptography** **14. Industrial Control System** 15. User Experience/Human Computer Interface Security **16. Offensive Cyber Operations** 17. Hardware Reverse Engineering

3. RELATED WORK

Developing a Cyber Science curriculum with content in-step with current industry needs while maintaining ABET accreditation and staying within institutional credit requirement constraints presents a challenge. Harris and Patten University of South Carolina (USC) formed an "IT Security-related and Cybersecurity Curriculum Taxonomy" to vertically integrate cybersecurity topics at appropriate course skill level including within core introductory courses. Harris and Patten advise that the human remains the weakest link and educational institutions must deliver cybersecurity knowledge to all graduates as they will likely enter a workforce that demands cyber hygiene from all.

Two interesting distinctions are 1) USC's focus is on information technology (IT) whereas USAFA's is on active cyber operations and 2) their taxonomy integrates cybersecurity into an existing computing curriculum whereas USAFA's cyber science curriculum is a distinct program separate from computer science. USAFA's cyber science integration does include teaching cybersecurity content including personal computing security within our core CS110 course. Harris and Patten also point out that failure to use a defined approach or taxonomy may lead to too much or not enough of appropriate breadth and depth of cybersecurity topics. Vertical integration and appropriate coverage and depth of cyber security to non-cyber security related disciplines is an open challenge at USAFA as we evaluate multiple options such as potentially adding a beyond 100-level core cyber science course for all cadets (Harris & Patten, 2015).

Rather than integrating IT-focused topics USAFA uses the National Security Agency's Center of Academic Excellence in Cyber Operations (CAE-CO) required knowledge units to inform content relevancy, depth, and breadth [9]. USAFA also uses Joint Task Force on Cybersecurity Education's "Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity." A recent Special Interest Group on Computer Science Education (SIGCSE) panel on cybersecurity education cites the NSA CAE-CO standards as well in the development of the JTF standard [10].

Cyber science education standards developed by ABET, ACM, NSA CAE-CO, and others recommend an interdisciplinary approach encumbering computer science educators budding cyber science programs with a unique challenge. Ramirez contends that cybersecurity is no longer a "technical subfield of computer science." He recommends a curriculum design approach which provides appropriate cybersecurity knowledge to non-cyber professionals and interdisciplinary studies in policy, computer science, management, and social science to cyber professionals. As a military institution, it is critical to recognize the differences in the government's use of cyber versus the non-government

sector's use. However, all cyber professionals usually communicate with non-cyber professional management and must learn effective communication skills within an effective cyber science education. USAFA's curriculum addresses providing a cyber education experience for non-cyber professionals as well as an emphasis on effective communication to both technical and non-technical audiences (Ramirez, 2017).

Bilzor advocates for a balanced approach to cyber education including both theory and application in a connected way. For example, teaching the Bell-LaPadula (BLP) model is included in many cyber security courses and textbooks. However, Bilzor points out there are no reported vulnerabilities within the national vulnerability database regarding the BLP model within the year of publication (2015). Indeed, he submits that students should understand the technical implementation of a system more so than a theoretical model though the model may serve as important background. He also advocates that principles are enduring whereas tools are not. Tools should be relevant and current to facilitate understanding but not "taught to." Bilzor also discusses the NSA CAE-CO criteria and how it refocuses from traditional computer science theory into practical cyber science applications. USAFA also uses this standard as a guiding tool for a relevant cyber science curriculum in conjunction with the theoretical computer science curriculum. Ultimately, Bilzor advocates that educators should examine the inclusion of traditional computer science theory before integrating it into a cyber science curriculum. A relevant cyber science curriculum should be informed by theory, in touch with modern application and hands-on [11].

4. PROGRAM DESIGN

The heart of our Cyber Science program design consists of a mapping of the six ABET Student Outcomes to our core Computer Science course, CS 110, which is a CS 0.5 course for all cadets, and our 14 required major's courses in a purposeful and deliberate manner. We then use the NSA CAE-CO criteria to help drive the specific technical content within each of the courses while considering recommendations from other sources and research described in Sections 2 and 3. Our Cyber Science major's courses are listed below.

- CS 210 – CS1 course
- CS 220 – CS2 course
- ECE 281 - Digital Design & Computer Architecture
- Math 340 – Discrete Math
- ECE 382 - Embedded Computer Systems
- CyS 333 - Cyber Warfare
- CS 467 – Networks
- CS 431 - Cryptography
- CyS 334 - Cyber Defense
- CS 483 – Operating Systems
- CyS 435 - Cyber Operations
- ECE 348 - Telecommunications Principles
- CyS 438 & 439 – Cyber Science Capstones

Additionally, we include two academic options. One computer science option, which is most-commonly filled by artificial intelligence or mobile applications; and one policy option selected from Cyber Law, Space and Cyber Strategy for National Security, or Cyber Security Policy and Politics.

The three-course sequence designated by CyS was built to specifically address cybersecurity requirements and provide in-depth coverage of cybersecurity topics. Cyber Warfare covers cyber attacks and the technical knowledge to identify and weaponized vulnerabilities and how to mitigate them. Cyber Defense focuses on secure network design including formal methods and forensic techniques. Cyber Operations applies that knowledge to planning and executing offensive and cyber operations in an Air Force context and reinforces many of the non-technical considerations of cybersecurity including laws, ethics, international politics, etc. Other major's courses address cybersecurity topics at a level appropriate for both Computer Science and Cyber Science majors, while these courses reinforce the topics and go much deeper into the topics to fully address the NSA CAE-CO requirements and ABET Program Criteria.

Table 3 depicts our mapping of courses to Student Outcomes. Shading distinguish semesters progressing from freshman to senior years with fall and spring offerings (CS 110 can be taken either semester of freshman year). Course Assessment Plans (CAP) for each course articulate explicit Course Outcomes to realize these mappings. The Course Outcomes detail specific requirements of the course together with how the Course Outcomes will be developed and assessed. For Student Outcome #3 on Communications, entries with a 'W' indicate that written communications is the focus while an 'O' means oral presentations will be addressed. These Course Outcomes and their mapping to Student Outcomes articulate how courses will contribute to accomplishing the Student Outcomes.

Table 3: Mappings of Student Outcomes to Courses

Cyber Science Mappings	110	210	220	281	340	382	333	467	431	334	483	435	438	348	439
1) Analyze and identify solutions	X	X	X	X	X	X	X	X	X	X	X	X	X	**X**	X
2) Design, implement, and evaluate	X	X	X	X		X	X	X	X	X	X	X	X	**X**	X
3) Communicate effectively		W	W	W			O			W/O		W/O	W		O
4) Professional responsibilities (legal/ethical)		X	X				X	X	X	X	X	X	X	**X**	X
5) Function effectively on a team		X	X				X	X		X		X	X		X
6) Apply security principles/practices	X	X	X			X	X	X	X	X	X	X	X	**X**	X

The CAPs for each course define specific student assessment mechanisms with threshold values for Met, Marginally Met, and Not Met. At the conclusion of each course offering, the Course Director writes a Course Assessment Report that includes the specific Course Outcome assessment results by each instrument used. The data from these assessments allows the department to make targeted changes to the course material and instructional methods to better meet the Course, Student, and Institutional Outcomes. Our annual Computer Science program assessment process utilizes Course Outcome assessments together with other quantitative and qualitative measures to assess our Student Outcomes. We dual-purpose selected Course Outcome assessments providing these results to Institutional Outcome Teams that consolidate measures from across disciplines for their assessment purposes. With this approach, our departmental assessment efforts can satisfy multiple assessment purposes based primarily on Course Outcome assessment results. One of the key benefits of aligning the outcomes is that it significantly reduces the administrative and reporting burden of assessing courses against outcomes from multiple sources and allows instructors to spend that regained time to apply the assessment results to improving and enhancing their courses.

5. ADDRESSING THE STUDENT OUTCOMES

The Cyber Science program's design centers on how we address the ABET Student Outcomes (SOs) and how they are applied and assessed across the program's courses. In this section, we provide specific examples of how we implemented the outcomes across our program's design. Within each course, we define and require coverage of particular topics and development of key skills and abilities facilitating a carefully woven curriculum that can be sustained across faculty changes while enabling the well-organized evolution needed in a rapidly changing discipline. This process can be utilized by other institutions to facilitate designing their programs and seeking accreditation.

5.1 Student Outcome #1 - Analyze and Identify Solutions

Beginning with our core-for-all CS 110 course, cadets are assigned a programming project that is typically a game or graphical simulation where the requirements are well-defined. The students focus on understanding formal requirements and applying what they have learned about programming to implement their project. With our CS 1-2 foundational programming course sequence (CS 210, CS 220), we start by providing well-stated formal requirements,

but in later assignments, we purposefully inject omissions, contradictions, and ambiguities into the problems explicitly soliciting the students' analyses and questions. If necessary, we employ the Socratic Method to draw them into discovering the right questions to ask and consider when evaluating requirements.

In the Cyber Warfare course, we introduce cadets to multiple types of software and network vulnerabilities through analysis and reverse engineering. The students must then propose a solution to patch the vulnerability as well as assess the proposed solutions of others in the class. In Cyber Defense, we analyze formal security models and principles, and then cadets are required to design a network using this information to meet multiple different missions and risk areas. The cadets then discuss the pros and cons of each proposed design. This development culminates with the senior year two-semester Cyber Science Capstone sequence where the students work in teams of four to six members to develop complex systems for real clients.

5.2. Student Outcome #2 - Design, Implement, and Evaluate

Cadets in the Cyber Science program develop their ability to design, implement, and evaluate solutions in both hardware and software. As described above, the cadets begin solving problems during the foundational programming courses. They continue building these skills in the Electrical and Computer Engineering (ECE) courses, as they design and build digital logic circuits and solve problems using embedded processors and hardware. In these ECE courses, cadets complete multiple labs where, after designing a solution, they must implement the hardware physically, or code the solution on a field programmable gate array. Another lab requires cadets to modify a MIPS processor with new hardware to add new instruction types previously not implemented. In Cyber Operations, cadets are given multiple scenarios and must design a solution considering the technical, legal, and policy constrains, brief it to their instructor, implement it, and finally evaluate how their solution worked or if it did not, how they had to modify their actions to reach the goal.

These courses provide the cadets with a foundational understanding of how to solve problems with a variety of programming and hardware design techniques. The cadets then apply these techniques in their two-course capstone projects. Every Cyber Science major participates in a two-semester capstone class where they are provided with a real-world, open-ended research, design, or engineering problem to solve. The cadets must use their knowledge to determine the best approach to solve the problem and then work as a team to implement their solution. Over the course of the two semesters, the cadets evaluate the effectiveness of their approach and their progress towards their goal and make adjustments as necessary. This allows the cadets to better understand real-world design problems where the end solution is not known or a viable solution may not even exist.

5.3. Student Outcome #3 - Communicate Effectively

Upon graduation, USAFA cadets will commission as Air Force officers, where they will need the ability to clearly communicate, regardless of their specific assignment. USAFA emphasizes Clear Communication as one of its nine intuitional outcomes, which are developed through our extensive 29-course core curriculum. We approach this by designating specific courses to address written or oral communications such that at least one course addresses communications from their first semester in the major (sophomore fall) through their last. In each of the final three semesters, we address both written and oral communications to ensure cadets internalize these skills.

We reinforce this institutional and student outcome in several major's courses, particularly in the three-course Cyber Science sequence and two capstone courses. In Cyber Warfare, cadets are required to provide a briefing on a technical vulnerability and mitigations for it. Additionally, they write a detailed technical report on a piece of malware they analyze and reverse engineer. Cadets create similar reports in Cyber Defense, where they write reports detailing their

forensic analysis of multiple systems. Cyber Operations dedicates approximately half of the class to planning, briefing, executing, and debriefing a series of missions, where the cadets not only brief their initial plan but also brief how the execution of the mission either matched or deviated from that plan. The cadets continue developing these skills in their capstone courses as they work in teams to design and implement solutions to real-world problems. They document their progress through oral status updates each lesson and formal briefings and reports at the end of each ten-lesson development sprint.

5.4. Student Outcome #4 - Professional Responsibilities

Our department has employed a long-standing tenant of "Ethics across the Curriculum." Each course in the department is required to include at least one lesson addressing a discipline-relevant ethical topic. Our CS1 and CS2 courses cover the ACM Code of Ethics and Professional Conduct [12] and several ethical frameworks. Introducing these in the first courses in the major provides the opportunity to use the ACM Code in subsequent courses as well as emphasizing its importance to the discipline. Due to the complexity of ethics and legal considerations in cybersecurity, each of the courses in the three-course Cyber Science sequence dedicates significant time throughout the course to discuss these issues. Cyber Warfare discusses the legal and ethical implications of reverse engineering and vulnerability research and the roles of "white hat" and "grey hat" hackers in cybersecurity. Cyber Defense reinforces the legal and ethical responsibilities of forensics investigators, covering applicable laws and the necessity of forensic examiners to remain unbiased and follow the evidence wherever it may lead. Students are required to demonstrate their understanding by applying these standards to forensics exercises, representative of a criminal investigation or incident response. Cyber Operations requires cadets to consider the legal and ethical aspects of Just War in planning and evaluating mission plans. The cadets must balance the potential military advantages against the potential for collateral damage or damage to civilian networks.

5.5. Student Outcome #5 - Function as a Team

USAFA focuses on developing future officers with leadership, teamwork, and organizational management skills as another institutional outcome. Cadets develop these skills daily as they live and work within their cadet squadrons, groups, and wing. These organizations mirror the operational Air Force chain of command with cadets leading at all levels. The cadets are responsible for executing numerous military duties and responsibilities such as inspections, parades, and athletics/intramurals, all of which require the cadets to work successfully as both small and large teams.

We reinforce this institutional and student outcome throughout the Cyber Science curriculum, with nine core major classes utilizing small group projects. We teach pair programming and divide and conquer strategies in our CS1 and CS2 courses and reinforce these methods in subsequent courses. In our Cyber Warfare and Cyber Defense courses, cadets work in teams of two or three members to reverse engineer a piece of malware or to perform a forensic examination of a small network. In Cyber Operations, a team of three will work through multiple simulated cyber operations, with each person taking a turn as Team Lead, Intelligence Officer, or Cyber Operator. In the Cyber Science capstone courses, team size grows to four to six students employing agile development methods, such as SCRUM, with each person assuming the role of team lead for at least one development sprint. This full-year capstone event provides the cadets with an opportunity to develop these skills in a real-world setting. Not only are they graded on the technical progress of their project, but they also are evaluated and given feedback on their team processes and dynamics. The teams must manage their resources including time and team-member skills to complete the project successfully.

5.6. Student Outcome #6 - Apply Security Principles & Practices

In addition to our core CS110 course, which dedicates eight lessons covering basic security principles and the cyber attack methodology, we primarily address the cybersecurity-specific student outcome through the three-course Cyber Science sequence. The sequence delivers theoretical knowledge as well as the opportunity to practice practical skills required of cyber science professionals, especially those positioned to lead within the United States military.

Cyber Warfare includes fundamental security design principles, low level programming (assembly language) application and programming security, reverse engineering, computability, and ethics. The course goes into detail regarding common software vulnerabilities and ways to both exploit and correct the vulnerabilities. Cadets must identify and exploit buffer and integer overflows, timing attacks including race conditions, and command injection before learning how to mitigate the vulnerabilities via secure programming practices. The last half of the course is dedicated to malware reverse engineering, building upon earlier programming knowledge as well as providing a preview to networking and operating system courses. Students are expected to understand Windows and Linux user-space malware, complete behavioral analysis both statically and dynamically, and deliver security recommendations.

Cyber Defense analyzes formal security models and how to use them to build resilient and secure systems and networks. Additionally, the cadets learn and demonstrate computer and network forensics techniques to recognize and recover from attacks. The course also emphasizes the importance of cyber intelligence to tailor defensive operations against expected threats and risks. Cyber Operations focuses on having cadets apply these skills to representative cyber attack and cyber defense scenarios. The cadets must analyze the scenarios including the mission objectives, threats, and risks, and then develop and execute a plan to successfully complete the missions. The missions are modeled to represent potential real-world missions with complex technical, legal, and political factors to consider, requiring the students to demonstrate a comprehensive understanding of cybersecurity concepts.

6. CONCLUSION

While this new Cyber Science program design is still in the process of implementation, it is based on a foundation of an already successful cybersecurity degree program that has been available at USAFA since 2014 and has been recognized as a National Security Agency Center of Academic Excellence in Cyber Operations. Keys to success will be continued institutional and departmental leadership support as well as a culture of purposeful curriculum design and continual assessment-based evolution. The main challenges include maintaining a disciplined and systematic process for curriculum change to respond and stay current in a rapidly changing discipline, keeping grading and assessment burdens efficient and manageable, and staying aligned with operational Air Force needs while also meeting our many guidance and accreditation sources. This paper described the process that we use to address those challenges. We align our course outcomes to ABET Student Outcomes to ensure we are properly preparing cadets to be future leaders and cybersecurity professionals. We also use the NSA CAE-CO requirements to inform the specific technical content within each course and address the ABET Program Criteria. Aligning these requirements allows us to more easily assess our courses and how well they are meeting objectives. Alignment also allows USAFA to better prepare our graduates to serve as future Air Force leaders with technical and critical thinking skills to meet the demands of our nation.

7. REFERENCES

[1] S. Lingafelt, "The History and Development of a “Cyber Security” Program Criteria," 11 November 2017. [Online]. Available: https://www.abet.org/the-history-and-development-of-a-cyber-security-program-criteria/.

[2] ABET, "ABET Approves Accreditation Criteria for Undergraduate Cybersecurity Programs," 30 November 2018. [Online]. Available: https://www.abet.org/abet-approves-accreditation-criteria-for-undergraduate-cybersecurity-programs/.

[3] ABET Computing Accreditation Commission, "Criteria for Accrediting Computing Programs," 29 October 2016. [Online]. Available: https://www.abet.org/wp-content/uploads/2016/12/C001-17-18-CAC-Criteria-10-29-16-1.pdf.

[4] ABET Computing Accreditation Commission, "Criteria for Accrediting Computing Programs," 12 February 2018. [Online]. Available: https://www.abet.org/wp-content/uploads/2018/02/C001-18-19-CAC-Criteria-Version-2.0-updated-02-12-18.pdf.

[5] ABET Computing Accreditation Commisson, "Criteria for Accrediting Computing Programs," 24 November 2018. [Online]. Available: https://www.abet.org/wp-content/uploads/2018/11/C001-19-20-CAC-Criteria-11-24-18.pdf.

[6] United States Air Force Academy, "Outcomes," 2019. [Online]. Available: https://www.usafa.edu/academics/outcomes/.

[7] Joint Task Force on Computing: Curricula Association for Computing Machinery (ACM) and IEEE Computer Society, "Computer Science Curricula 2013, Curriculum Guidelines for Undergraduate Degree Programs in Computer Science," 20 December 2013. [Online]. Available: https://www.acm.org/binaries/content/assets/education/cs2013_web_final.pdf.

[8] Joint Task Force on Cybersecurity Education, "Cybersecurity Curricula 2017, Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity," 31 December 2017. [Online]. Available: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf.

[9] National Security Agency, Central Security Service, "Criteria for Measurement for CAE in Cyber Operations Fundamental," [Online]. Available: https://www.nsa.gov/Resources/Students-Educators/centers-academic-excellence/cae-co-fundamental/.

[10] R. K. Raj, V. Anand, D. Gibson, S. Kaza and A. Phillips, "Cybersecurity Program Accreditation: Benefits and Challenges," *SIGCSE '19 Proceedings of the 50th ACM Technical Symposium on Computer Science Education,* pp. 173-174, 2019.

[11] M. Bilzor, "Seeking Balance in Cyber Education," US Naval Academy, 2015.

[12] Association of Computing Machinery, "ACM Code of Ethics and Professional Conduct," 22 June 2018. [Online]. Available: https://www.acm.org/code-of-ethics.

[13] M. Harris and K. Patten, "Using Bloom's and Webb's Taxonomies to Integrate Emerging Cybersecurity Topics into a Computing Curriculum," *Journal of Information Systems Education,* vol. 26, no. 3, pp. 219-234, 2015.

[14] R. B. Ramirez, "Making cyber security interdisciplinary : recommendations for a novel curriculum and terminology harmonization," Massachusetts Institute of Technology, Massachusetts Institute of Technology, 2017.

[15] J. Marquardson and D. L. Gomillion, "Cyber Security Curriculum Development: Protecting Students and Institutions While Providing Hands-On Experience," *Information Systems Education Journal,* vol. 16, no. 5, pp. 12-21, October 2018.

[16] F. J. Sheen, "An Extensible Technology Framework for Cyber Security Education," Brigham Young University - Provo, 2015.

[17] National Security Agency, Central Security Service, "Centers of Academic Excellence in Cyber Operations," [Online]. Available: https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-centers/.