Holistic Cyber Education

Jean R.S. Blair, Andrew O. Hall, and Edward Sobiesk[1]

Cyber has permeated all aspects of our lives and society. Consequently, it is a moral imperative that cyber be integrated into all levels of education. This paper provides a multi-level, multidisciplinary approach for holistically integrating cyber into a student's academic experience. Our approach suggests formally integrating cyber throughout an institution's curriculum, including within the required general education program, in electives from a variety of disciplines, as multi-course threads, as minors, and in numerous cyber-related majors. Our holistic approach complements in-class curricula with both a pervasive cyber-aware environment and experiential, outside-the-classroom activities that apply concepts and skills in real-world environments. The goal of our approach is to provide all educated individuals a level of cyber education appropriate for their role in society. Throughout the description of our approach, we include examples of its implementation at the United States Military Academy (USMA).

Throughout this paper we use the term cyber, but we acknowledge the ambiguity and open-endedness of the term. One current, popular definition of cybersecurity is:

> *A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management (ACM 2017b).*

While this definition describes much of what we mean by the term, we broaden the concept to include the full multidisciplinary technical and non-technical aspects of cyber.

The next section describes the most relevant related work. This is followed by sections that respectively address recommended curricular and extracurricular elements of our approach. A final section describes the importance of a pervasive cyber-aware environment.

[1] The views expressed in this article are those of the authors and do not reflect the official policy or position of the U.S. Military Academy, the Department of the Army, the Department of Defense, or the U.S. Government.

Related Work

This section briefly highlights the primary related work for teaching cyber, which we organize into the following categories:

- Computer security in traditional computing curricula
- NSA/DHS designations
- ABET accreditation criteria
- Standalone cybersecurity curriculum and accreditation criteria
- Cyber in general education and electives
- Extracurricular cyber opportunities

Computer security in traditional computing curricula. Professional societies for computing, including the Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS), and the Association for Information Systems (AIS), have created curricular guidelines for Computer Science (2013), Information Systems (2010), Information Technology (2017), Computer Engineering (2016), and Software Engineering (2014). These model curricula provide frameworks that influence hundreds to thousands of computing programs across the United States and internationally. Each of these model curricula contains recommended computer security content for the associated discipline, under labels such as Information Assurance and Security, Cybersecurity, and Information Security. These computer security curricular recommendations are usually meant to be taught across the program's entire curriculum rather than just in a single course. As example, the Computer Science model curriculum recommends 9 lesson hours of "concepts where the depth is unique to Information Assurance and Security" and an additional 63.5 lesson hours of Information Assurance and Security content that is "integrated into other Knowledge Areas that reflect naturally implied or specified topics with a strong role in security concepts and topics" (ACM 2013). The content for these curricular recommendations is mostly technical material that applies to the part of the curriculum being covered. Thus, an agreed upon best practice at the program level for computing disciplines is to teach cybersecurity across the entire breadth of the curriculum rather than only bolted-on to the curriculum in a single course.

NSA/DHS designations. Additional computing program level initiatives include the National Security Agency and the Department of Homeland Security jointly sponsoring the National Centers of Academic Excellence in Cyber Defense (CAE-CD) program that offers CAE CDE designations for Associate, Bachelor, Masters and Doctoral Programs (2020). The CAE-CD program's goal is to "reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise" (NSA 2020). Complementing this, the National Security Agency additionally sponsors the National Centers of Academic Excellence (CAE) in Cyber Operations Program (2020) that supports the National Initiative for Cybersecurity Education (NICE) Framework (2019). The CAE-Cyber Operation's intent is to facilitate curricula that meet the goal of being a "deeply technical, inter-disciplinary, higher education program firmly grounded in the computer science, computer engineering, and/or electrical engineering disciplines, with extensive opportunities for hands-on applications via labs and exercises" (NSA 2020). Currently, there are over 300 institutions with the CAE in Cyber Defense designation and 21 institutions with the CAE in Cyber Operations designation (NSA 2020).

ABET accreditation criteria. For program-level computing accreditation, ABET accredits hundreds of traditional computing programs across the United States and internationally. ABET has recently changed their computing accreditation criteria, and starting in the 2018-2020 time period, all computing programs seeking accreditation or reaccreditation will have to demonstrate that they have curriculum content that sufficiently covers "principles and practices for secure computing" appropriate to their discipline (ABET 2020).

Standalone cybersecurity curriculum and accreditation criteria. From the viewpoint of cybersecurity as a distinct discipline, and not simply an aspect of a computing discipline, a Joint Task Force on Cybersecurity Education, comprised of four professional societies (Association for Computing Machinery, IEEE Computer Society, Association for Information Systems Special Interest Group on Security, and International Federation for Information Processing Technical Committee on Information Security Education), published *Cybersecurity Curricula 2017* (CSEC2017). Its vision is, "The CSEC2017 curricular volume will be the leading resource of comprehensive cybersecurity curricular content for global academic institutions seeking to develop a broad range of cybersecurity offerings at the post-secondary level" (ACM 2017b). The guidelines frame cybersecurity through three dimensions: crosscutting concepts, knowledge areas, and disciplinary lenses. The six crosscutting concepts are Confidentiality, Integrity, Availability, Risk, Adversarial Thinking, and Systems Thinking. The eight knowledge areas include Data Security, Software Security, Component Security, Connection Security, System Security, Human Security, Organizational Security, and Societal Security. The disciplinary lenses represent "the underlying computing discipline from which the cybersecurity program can be developed….The thought model encompasses the current computing disciplines identified by the ACM: computer science, computer engineering, information systems, information technology, and software engineering" (ACM 2017b). Based on *Cybersecurity Curricula 2017* and on constituent needs, ABET has recently developed, published, and fielded cybersecurity program criteria (ABET 2020).

Cyber in general education and electives. Few institutions require cybersecurity as part of their general education program. However, a few do. Examples of such requirements include mandated general education courses at the United States Military Academy (Sobiesk et al 2015) and the United States Naval Academy (Brown et al 2012). Examples of cyber electives and cyber minors are found in (Sobiesk et al 2015) and (Stockman et al 2006).

Extracurricular cyber opportunities. Outside the classroom, there are extracurricular competitive opportunities, training courses that often have associated certifications, and government frameworks. Three well known educational extracurricular cybersecurity competitions are the college-level National Collegiate Cyber Defense Competition (2020) that includes roughly 200 institutions, CyberPatriot (2017) which includes 3000+ teams composed of high school and middle school students, and PicoCTF (2017) "a game designed to expose students to the science of computer security," which has over 17,000 middle and high school participants. Additionally, SANS CyberStart provides "a suite of challenges, tools and games designed to introduce young people to the field of cyber security" (SANS 2020). Hundreds of capture the flag competitions also take place every year in which competitors are faced with a plethora of real world, concrete instances of computer security challenges (CTFtime.org 2020). Hundreds of cybersecurity conferences also take place every year, providing scholars and the private sector chances to share ideas, innovations, and research (Concise AC 2020). There are numerous training courses and certifications associated specifically with cybersecurity or that include significant security components. Some of the most prominent come from organizations such as SANS (2020), ISC2 (2020), Cisco (2020), and ISACA (2020).

Curricular Elements of the Holistic Approach

The primary contribution of this paper is a holistic, multi-level, multidisciplinary approach that provides all individuals a level of cyber education appropriate for their role in society. This model integrates and significantly builds on our previous work (Sobiesk et al 2015; Hall and Sobiesk 2017; Blair et al 2019). In the curricular elements of our approach, cyber education includes technical and non-technical content across the various levels, which include:

- general education content – giving all students the basics of cyber
- disciplinary and interdisciplinary cyber electives, in areas like Political Science, Law, Cognitive Science, and Computing – providing opportunities to supplement one's education with cyber-related content
- elective or embedded-in-a-major cyber-focused threads, such as cybersecurity engineering or robotics – providing the opportunity to specialize in cyber at a level less than a minor but more than a single course
- cyber minors – including both technical and non-technical knowledge areas
- technical and non-technical cyber-related majors that prepare graduates to succeed in the Cyber Domain

Figure 1, inspired by (Sobiesk et all 2015), illustrates the various curricular levels of this approach. In the subsequent sections, we elaborate on each of the levels in detail as well as provide examples.

Cyber in General Education

We believe all educated individuals need at least a fundamental level of cyber education. To that end, we advocate integrating cyber into general education requirements. The key pedagogical technique is to consciously make cyber literacy and cybersecurity an institutional goal. With that, it becomes easier to purposely integrate cyber into as many places as possible in the general education curriculum and to ensure that every student's path includes sufficient coverage. This obviously includes computing and other Science, Technology, Engineering and Mathematics (STEM) disciplines, but cyber should also be addressed when covering most of the social sciences (such as political science, economics, international relations, and sociology) as well as in law, ethics, and social justice components, and in studies of human behavior.

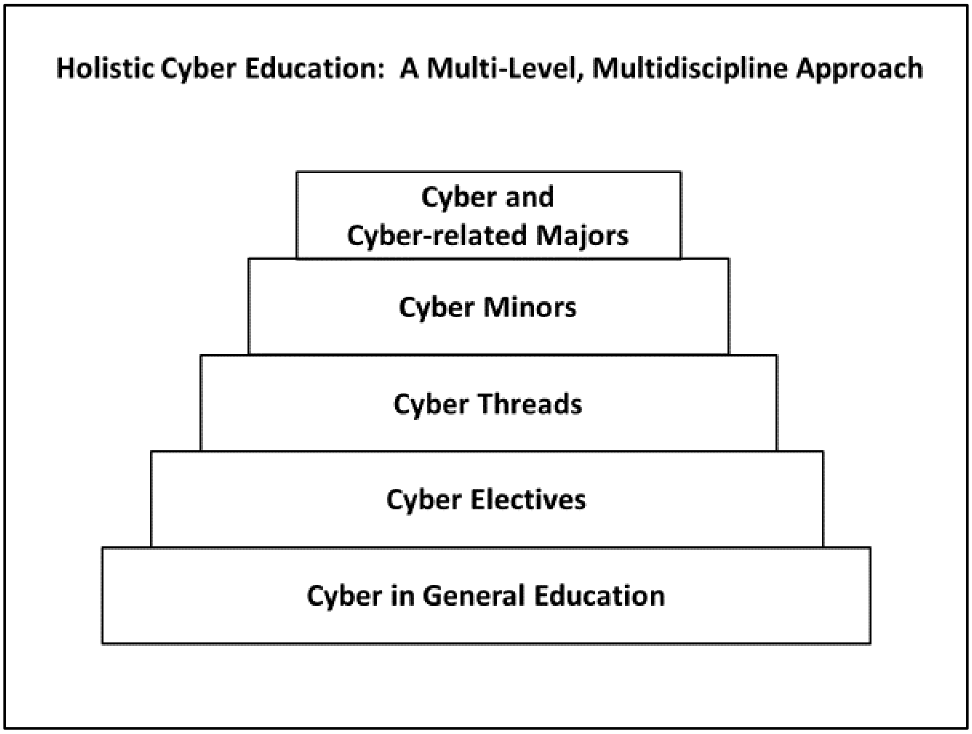
Holistic Cyber Education: A Multi-Level, Multidiscipline Approach
Cyber and
Cyber-related Majors
Cyber Minors
Cyber Threads
Cyber Electives
Cyber in General Education

Figure 1: Curricular elements of the holistic cyber education approach.

We realize that general education requirements will vary greatly by institution, with the USMA's being among the most stringent in the world. However, we believe that the concepts and vision illustrated through the following examples can provide inspiration and exemplars for almost any institution.

During their four academic years in attendance at the USMA, all cadets must complete a minimum of 40 academic courses, of which 27 are core general education courses spanning a variety of disciplines, including numerous courses in the humanities, social sciences, and STEM disciplines. Each cadet also chooses a major from across the same spectrum, but the core STEM requirements are so rigorous that all cadets, regardless of their chosen major, receive a Bachelor of Science degree.

There are two core general education courses assigned to specifically introduce cadets to computing and the cyber domain. The first course, CY105 Computing Fundamentals, introduces the principles and practices of computing along with foundational design and construction techniques for computer programming. The course also covers "legal, ethical, professional, and security issues and the challenges, opportunities, and attributes of the Cyber Domain" (United States Military Academy 2016). A second core course, CY305 Cyber Foundations, provides cadets the "capacity and confidence to employ information technology – hardware, software, and networks – to empower people and organizations to acquire, manage, communicate and defend information, solve problems, and adapt to change. It provides a deeper understanding of sensor and communications technologies; computer processing, storage, and networks; cyberspace operations, planning and management; interaction of components in Cyberspace; data-driven decision making; and the evolving legal and ethical framework surrounding use of IT and operating in the cyber domain. Cybersecurity issues are addressed throughout the course" (United States Military Academy 2016). All cadets take the first course and get the content from the second course either by taking the course itself or by completing an engineering or computing major that provides equivalent content.

Several additional courses contribute to the integration of cyber across the USMA's general education curriculum. As examples, a required Probability and Statistics course exposes cadets to scripting, command line interface, and open source software as a part of coding in the R statistical language, and required courses in International Relations, Economics, Law, and even History and Philosophy, address the evolving aspects of those disciplines that are becoming interwoven with Cyber as a Domain. All this content is required as a part of the liberal education taken by all cadets and supports the Academy's goal that all graduates are able to "explain and apply Computing and Information Technology concepts and practices in the context of the Cyber Domain" (United States Military Academy 2016).

The USMA is continuing to evolve the integration of cyber across the required general education curriculum at West Point. Members of the USMA's faculty from many departments are working together to integrate content and concepts involving the Cyber Domain without adding additional required courses. We believe cooperation across disciplines is an essential element to holistically integrating cyber content into general education at any institution.

Cyber Electives in a Variety of Disciplines

Cyber electives increase accessibility to the subject, providing greater depth across a variety of disciplines. In our experience, this inspires a wider range of students to explore and learn about cyber from numerous valuable perspectives. It also naturally creates opportunities for students to develop multidisciplinary collaborative skills and mindsets.

The USMA offers many cyber electives as well as independent study opportunities. Cyber electives are offered in computing disciplines, interdisciplinary domains, and non-computing disciplines. Popular cyber electives include (United States Military Academy 2016):

- Computer Science course CS483 Digital Forensics
- Computer Science Special Topics course CS485 Ethical Hacking
- Cyber Engineering course CY450 Cyber Security Engineering
- Cyber Science course CY383 Secure Interface Design
- Cyber Science course CY460 Cyber Policy, Strategy & Operations
- Electrical Engineering Special Topics course EE485 Hardware Hacking
- Engineering Psychology course PL475 Human-computer Interaction
- History course XH341 Intelligence Cyber History
- Information Technology Special Topics Course IT485 Principles of Intelligence Analysis
- Law course LW462 Cyber Law
- Math course MA464 Applied Algebra with Cryptology
- Philosophy course PY326 Cyber Ethics

In addition to the cyber electives, cadets completing a cyber-related major can also choose a cyber topic for their senior capstone design experience. A recent example of a successful cyber-related capstone project was a cadet team that designed and built a "Vulnerable Web Server application … that packages instructional materials and pre-built virtual machines, created using Oracle VirtualBox, into interactive cybersecurity lessons" designed for non-computing high school and college students (Estes et al 2016).

Cyber Threads

We define a thread to be a series of related courses that includes more than a single elective, but less than a minor. A thread provides opportunities for the students who do not have room in their schedule for a full minor but want greater study-in-depth in a discipline other than their chosen major.

The USMA curriculum offers each cadet the opportunity to experience an engineering thread as part of their education, ensuring exposure to the engineering thought and design process. For cadets in an engineering or computing major, this engineering sequence content is part of their major's required courses. The remainder of cadets, however, are required to take a three-course thread in addition to their major. One of these three-course threads is Cyber Engineering. The Cyber Engineering Thread is as follows (United States Military Academy 2016).

- CY300 Programming Fundamentals covers “fundamental computing concepts that will allow them to design, build and test small to medium programs using a high-level programming language.”
- CY350 Network Engineering and Management “addresses the analysis, design, building, and testing of modern computer networks.”
- CY450 Cyber Security Engineering teaches cadets to “design, build and test secure networked computer systems” including a “hands-on experience with current network security tools and techniques” and a culminating exercise where cadets “design, build and test defensive measures to protect a production network from intrusions”.

Essentially, the Cyber Engineering Thread can be viewed as (1) programming, (2) networking, and (3) securing.

Cyber Minors

A cyber minor is typically a set of related courses that together provide a depth of study that is not quite as extensive as a cyber major, but involves more courses, and is typically a more purposeful learning experience, than a thread. A cyber minor often may be used to complement an academic major or to enrich the interdisciplinary experience. Similar to electives, a cyber minor inspires a wide range of students with various backgrounds to study cyber from diverse academic perspectives. A cyber minor will, by its nature, encourage students to take courses across multiple disciplines and to develop multidisciplinary collaborative skills and mindsets.

At the USMA, a stated goal for the Cyber Security Minor is to achieve a “balance of both technical and non-technical knowledge and skills, as well as application” (United States Military Academy 2016). The minor builds on the Cyber Engineering Thread by requiring the two technical courses CY350 Network Engineering and Management and CY450 Cyber Security Engineering discussed above. Note that in preparation for these two courses, cadets must have taken the two cyber general education courses and CY300 Programming Fundamentals. In addition to the technical component of the Cyber Security Minor, a non-technical course must be chosen from the following three: CY460 Cyber Policy, Strategy & Operations, LW462 Cyber Law, or PY326 Cyber Ethics. Two additional elective courses are required from an extensive number of possibilities across a spectrum of disciplines.

Cyber-Related Majors

Cyber-related majors fall into three general categories: a stand-alone cyber major, cyber-related technical majors, and cyber-related non-technical majors. The technical and non-technical cyber-related majors are generally traditional majors that posses the potential to be cyber-related, depending on the focus of the curriculum or the student’s curricular choices.

- A stand-alone cyber major is usually computing-based, having one of the computing disciplines as its foundation, and covers much of the multidisciplinary content described in CSEC2017, which we summarized in the Related Work section. Examples of stand-alone cyber majors include cybersecurity, cyber operations, computer security, information assurance, information security, and computer forensics.
- A cyber-related technical major is often computing-based, but also includes a significant variety of other STEM majors. Examples of cyber-related technical majors include: computer science, information technology, information systems, computer engineering, software engineering, electrical engineering, physics, mathematics, operations research, systems engineering, artificial intelligence, and data science.
- A cyber-related non-technical major encompasses a vast spectrum of other contributing disciplines. Examples of cyber-related non-technical majors include: political science, international relations, cognitive science, psychology, philosophy/ethics, law, and criminal justice.

At the USMA, we have all three categories of majors.

The USMA Cyber Science major is consistent with CSEC2017 and consists of the following five concentrations that share a ten-course common foundation (United States Military Academy 2016).

- The Cybersecurity concentration focuses on "the interdisciplinary study of people, processes, and technology to assure operations in the face of cyberspace risks."
- The Network Services concentration focuses on "building and securing the networks and services that are foundational to operating in Cyberspace."
- The Cyber Operations concentration focuses on "the low-level and technical skills that enable offensive and defensive cyberspace operations."
- The Cyber-Physical Systems concentration "provides a unique blend of depth in both hardware and software to exploit networked, physical systems that are controlled by algorithms."
- The Machine Learning concentration focuses on gaining insight using algorithmic tools that exploit large datasets and the Internet-of-Things.

The USMA's cyber-related technical majors include Computer Science, Electrical Engineering, Mathematical Sciences, Operations Research, Applied Statistics and Data Science, Physics, Systems Engineering, Engineering Management, and Systems and Decision Sciences. The USMA's cyber-related non-technical majors include Psychology, Engineering Psychology, Law and Legal Studies, Political Science, International Relations, Philosophy, and Defense and Strategic Studies. In addition, at the USMA many cadets that take a traditional major supplement it with either our Cyber Engineering Thread or our Cyber Security Minor.

Extracurricular Elements of the Holistic Approach

Outside the classroom experiences are a critical component of a holistic cyber education approach. These activities provide experiential learning opportunities to apply concepts and skills from the classroom in a real-world environment. These experiences also offer the chance for developing communication, team work, and professional judgment skills as well as hands-on training experiences not always available in an educational environment. Outside the classroom cyber opportunities include internships, part-time jobs, research projects, student clubs, competitive events, conferences, training courses, and personal study.

At the USMA, cadets explore the cyber domain through participation in and attendance at cyber clubs, cyber-related conferences and training, summer internships across the U.S. Department of Defense and U.S. private sector, through short temporary assignment to a U.S. Army cyber unit, and with assigned mentors. The following paragraphs elaborate more of each of these USMA experiences.

The USMA has four cyber-related clubs:

- The Association for Computing Machinery Special Interest Group for Security, Audit and Control Club (SIGSAC) is open to all cadets with about 100+ participating. SIGSAC shares knowledge, cultivates technical skills, and develops leadership traits applicable to the Cyber Domain.
- The Cadet Competitive Cyber Team (C3T) consists of about 20 members selected through tryouts. They practice on an almost daily basis to prepare for, and compete in, numerous capture the flag competitions that improve their own computer and network security skills and serve as a form of outreach.
- The Cyber Policy Team is open to all cadets, with about 15 participating. This interdisciplinary club is dedicated to the study and application of cyber policy. The team competes at the regional, national, and international levels in various cyber policy competitions, including the annual Cyber 9/12 Student Challenge. The team's purpose is to encourage competition and a honing of cyber policy skillsets amongst our cadets.
- The Amateur Radio Club (HAMS) is open to all cadets, with about 50 participating. The goal of the club is to provide an educational environment which fosters enthusiasm for amateur radio and community service.

Several USMA cadets attend conferences such as ShmooCon, DEF CON - Black Hat, CyCon, and CyCon U.S. Attending these events allows cadets to encounter and interact with the larger cyber community of interest. In some cases, cadets even present results of their own research.

A few cadets participate in commercial cyber training with organizations such as described in the Related Work section. Other cadets experience cyber military training by either attending a military training course or by being assigned for a few weeks to a military cyber unit.

About 100 cadets participate each summer in cyber-related internships. All of these internships directly relate to the Cyber Domain, and many of them are associated with conflict in the Cyber Domain. As example, about 20 cadets conduct a summer internship with the NSA. Other cadet summer internships with a cyber focus include Facebook, USAA Cyber Operations Center, FBI, CERDEC, Lincoln Laboratories, and Amazon.

A Pervasive Environment

One of the most critical aspects of a student's developmental experience is exposure to the culture, environment, and role models that facilitate their growth into professionals and leaders who possess the character and competence required to succeed in and adapt to the Cyber Domain. This includes interacting with members of the faculty and profession to receive mentorship, career guidance, and perhaps, most importantly, inspiration.

Based on the USMA's unique mission and goals, about 25% of the faculty are civilian with the remaining 75% consisting of some of the Army's very best officers, with advanced degrees, and who represent all branches of the Army. Across this diverse and enthusiastic organization, the Army also made the decision to place the 70-person Army Cyber Institute at the USMA allowing for faculty with cyber expertise to be in at least nine different departments, and strongly contributing to the holistic, multidisciplinary cyber model adopted by the USMA.

The U.S. Army Cadet Cyber Development Program

As a closing note, Army ROTC and USMA cadets have the unique opportunity to formally synchronize and track their cyber activities as part of the U.S. Army's Cyber Leader Development Program (CLDP), which includes a formal mentorship program. As described at (Army Cyber Institute 2020), CLDP identifies, develops, and tracks cyber leaders and is encouraged for cadets taking cyber-related majors or a cyber minor. Overall:

> *CLDP provides a framework for cadets to pursue 800+ hours of impactful experiences outside the classroom through internships, conferences, clubs, and seminars. Cadets in CLDP pursue opportunities to attend advanced cyber training offered by SANS, Cisco, and other organizations….Cadets in CLDP will also be favorably considered for the most challenging, technical Academic Individual Advanced Development opportunities at organizations such as the NSA, U.S. Cyber Command, U.S. Army Cyber Command, and other institutions that have a cyber*

operations mission (Army Cyber Institute 2020).

Successful completion of the Cyber Leader Development Program results in the award of an Additional Skill Identifier on a cadet's permanent military record.

Conclusion

This paper addressed the moral imperative to integrate cyber into all levels of education – with the goal of providing all individuals a level of cyber education appropriate for their role in society. Towards this end, we described a holistic multi-level, multidisciplinary approach that incorporates the curricular and extracurricular elements of the student experience, complemented by a pervasive cyber-aware environment. While our approach and examples primarily focused on undergraduate education, we believe our principles and recommended practices easily extend to K-12 and graduate-level education.

REFERENCES

ABET. 2020. CAC General and Program Criteria. ABET. Baltimore, MD. http://www.abet.org

ACM. 2013. Computer Science Curricula 2013. ACM/IEEE-CS Joint Task Force on Computing Curricula. https://www.acm.org/education/curricula-recommendations

ACM. 2016. Curriculum Guidelines for Undergraduate Degree Programs in Computer Engineering. ACM/IEEE-CS Joint Task Force on Computer Engineering Curricula. https://www.acm.org/education/curricula-recommendations

ACM. 2010. Curriculum Guidelines for Undergraduate Degree Programs in Information Systems. ACM/AIS Joint IS 2010 Curriculum Task Force. https://www.acm.org/education/curricula-recommendations

ACM. 2017a. Curriculum Guidelines for Undergraduate Degree Programs in Information Technology. ACM/IEEE-CS Task Group on Information Technology Curricula. https://www.acm.org/education/curricula-recommendations

ACM. 2014. Curriculum Guidelines for Undergraduate Degree Programs in Software Engineering. IEEE Computer Society/ACM Joint Task Force on Computing Curricula. https://www.acm.org/education/curricula-recommendations

ACM. 2017b. Cybersecurity curricula 2017. Joint Task Force on Cybersecurity Education. https://www.acm.org/education/curricula-recommendations

Army Cyber Institute. 2020. Cyber Leader Development Program (CLDP) Overview. https://cyber.army.mil

BestColleges. 2020. The Best Online Bachelor's in Cybersecurity Programs of 2020. https://www.bestcolleges.com/features/top-online-bachelors-in-cybersecurity/

Blair, J., Hall, A., and Sobiesk, E. 2019. Educating Future Multidisciplinary Cybersecurity Teams. *Computer*. 52 (3)

Brown, C., Crabbe, F., Doerr, R., Greenlaw, R., Hoffmeister, C., Monroe, J., Needham, D., Phillips, A., Pollman, A. 2012. Anatomy, dissection, and mechanics of an introductory cyber-security course's curriculum at the United States naval academy. In *Proc. Conf. Innovation and technology in computer science education*. Haifa, Israel.

CISCO. 2020. CISCO Training and Certifications. https://www.cisco.com/c/en/us/training-events/training-certifications.html

Concise AC. 2020. Cybersecurity Conferences 2020 – 2021. https://infosec-conferences.com

CTFTime. 2020. https://ctftime.org

CyberPatriot. 2020. https://www.uscyberpatriot.org

Estes, T., Finocchiaro, J., Blair, J., Robison, J., Dalme, J., Emana, M., Jenkins, L., Sobiesk, E. 2017. A capstone design project for teaching cybersecurity to nontechnical users. In *Proc. Conf. Information Technology Education*. Boston, MA.

Hall, A. and Schultz, B. 2017. Direct Commission for Cyberspace Specialties. *Cyber Defense Review.* 2 (2)

Hall, A. and Sobiesk, E. 2017. Integration of the cyber domain at the United States Military Academy in *Proc. Int. Workshops: Realigning Cybersecurity Education*, Australia, 2017. doi: 10.1145/3293881.3295778

ISACA. 2020. https://www.isaca.org

ISC2. 2020. https://www.isc2.org

Nakasone, P. and Lewis, C. 2017. Cyberspace in Multi-Domain Battle. Cyber Defense Review. *Cyber Defense Review.* 2 (1)

National Collegiate Cyber Defense Competition. 2020. http://www.nationalccdc.org

NICE. 2019. NICE Cybersecurity Workforce Framework. National Initiative for Cybersecurity Education. https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

NSA. 2020. National Centers of Academic Excellence in Cyber Defense and in Cyber Operations. https://www.nsa.gov/resources/students-educators/centers-academic-excellence

Parrish, A., Impagliazzo, J., Raj, R.K., Santos, H., Asghar, M.R., Jøsang, A., Pereira, T., and Stavrou, E. 2018. Global perspectives on cybersecurity education for 2030: A case for a meta-discipline. In *Proc. Conf. Innovation and Technology in Computer Science Education.* Larnaca, Cyprus. 2018

picoCTF. 2020. https://picoctf.com

SANS. 2020. https://www.sans.org

Sobiesk, E., Blair, J., Conti, G., Lanham, M., and Taylor, H. 2015. Cyber education: A multi-level, multi-discipline approach. In *Proc. Conf. Information Technology Education.* Chicago, IL

Stockman, M., Leung, S., Nyland, J., and Said, H. 2006. The Information Technology Minor: Filling a Need in the Workforce of Today. In *Proc. Conf. Information Technology Education.* Minneapolis, MN

United States Military Academy. 2016. Academic Program - Class of 2020 Curriculum and Course Descriptions (RedBook). https://www.westpoint.edu/academics/dean/strategic-documents