Cyber Education: A Multi-Level, Multi-Discipline Approach

Edward Sobiesk, Jean Blair, Gregory Conti, Michael Lanham, and Howard Taylor
United States Military Academy
West Point, New York 10996 USA
edward.sobiesk, jean.blair, gregory.conti, michael.lanham, howard.taylor @usma.edu

ABSTRACT

The purpose of this paper is to contribute to the emerging dialogue on the direction, content, and techniques involved in cyber education. The principle contributions of this work include a discussion on the definition of cyber and then a description of a multi-level, multi-discipline approach to cyber education with the goal of providing all educated individuals a level of cyber education appropriate for their role in society. Our work assumes cyber education includes technical and non-technical content at all levels. Our model formally integrates cyber throughout an institution's entire curriculum including within the required general education program, cyber-related electives, cyber threads, cyber minors, cyber-related majors, and cyber enrichment opportunities, collectively providing the foundational knowledge, skills, and abilities needed to succeed in the 21st Century Cyber Domain. To demonstrate one way of instantiating our multi-level, multi-discipline approach, we describe how it is implemented at our institution. Overall, this paper serves as a call for further discussion, debate, and effort on the topic of cyber education as well as describing our innovative model for cyber pedagogy.

Categories and Subject Descriptors

K.6.m [**Miscellaneous**]:
Security
K.4.2 [**Social Issues**]:
Abuse and crime involving computers
K.3.2 [**Computer and Information Science Education**]:
Computer science education, Information systems education, Literacy

General Terms

Security, Management, Legal Aspects

Keywords

Cyber; cyber security; multi-level cyber education; multi-discipline cyber education; cyber education paradigm

1. INTRODUCTION

The purpose of this paper is to contribute to the emerging dialogue on the direction, content, and techniques involved in cyber education. Although several conferences now specifically focus on the topic of cyber education [1-3], it is also essential for the information technology (IT) education community to discuss and debate whether IT2008 curriculum guidelines [4] (specifically, the Information Assurance and Security (IAS) Knowledge Area within the IT body of knowledge) provide sufficient breadth and depth of coverage to address the emerging crises and opportunities in the area of cyber. This paper argues that the current IAS guidelines are not sufficient, and as a proposal for a broader perspective, presents a model of integrating cyber topics across all levels of the curriculum and into many non-computing disciplines.

The greatest contribution of this work is the presentation of a multi-level, multi-discipline approach to cyber education with the goal of providing all educated individuals a level of cyber education appropriate for their role in society. Specifically, our work describes a model of formally integrating cyber throughout an institution's curriculum including within the required general education program, in offerings of cyber elective topics in computing domains, interdisciplinary domains, and non-computing domains, in offerings of cyber threads and cyber minors, and finally in having major programs that provide foundational knowledge, skills, and abilities needed to succeed in the 21st Century Cyber Domain. To demonstrate one way of instantiating our multi-level, multi-discipline approach, we describe how it is implemented at the United States Military Academy at West Point. Following the discussion of our cyber-focused curricular experiences, we also briefly summarize our cyber enrichment opportunities, which we feel significantly complement the formal in-class instruction.

Before presenting this multi-level, multi-discipline approach, however, this paper discusses the greatly undervalued question of "what is cyber?", which is a critical question that needs to be addressed if the many ongoing initiatives involving cyber are ever going to converge to a successful, unified vision and effort.

Overall, this paper is a call for further discussion, debate, and effort on the topic of cyber education and for increased involvement by the IT profession in addressing cyber threats and opportunities.

2. WHAT IS CYBER?

Before describing our approach to cyber education, we believe there is value in first discussing the important unresolved question of what the term "cyber" means. Although cyber education, cyber programs, and cyber initiatives are growing at an almost exponential rate, there is not consensus on the meaning of the term cyber; in fact, it has many diverse interpretations based on the setting and constituents involved. This paper will not address all of the possible meanings. However, we will describe the definitions that have had the greatest impact on our own efforts.

SIGITE'15, September 30–October 3, 2015, Chicago, IL, USA.

ACM 978-1-4503-3835-6/15/09…$15.00.
http://dx.doi.org/10.1145/2656450.2656478

Perhaps the best known educational references to cyber are the two National Center of Academic Excellence (CAE) programs, one in Information Assurance/Cyber Defense and one in Cyber Operations, sponsored jointly by the National Security Agency and the Department of Homeland Security [5]. The CAE programs do not provide an explicit definition of 'cyber,' though the context of the certification programs makes the implicit linkage to networked computing systems clear. Currently, there are over 200 schools that hold a CAE certification of some kind.

Another well-known contemporary cyber effort is the Cyber Education Project (CEP) [6]. CEP is "an initiative supported by a diverse group of computing professionals representing academic institutions and professional societies to develop undergraduate curriculum guidelines and a case for accreditation for educational programs in the Cyber Sciences." Organized in July 2014, CEP is currently leveraging a community of interest to inform and drive this work forward. Their web site provides a useful review of existing cyber education efforts. They currently favor the term Cyber Sciences which they define as the following:

> The term "Cyber Sciences" reflects a collection of computing-based disciplines involving technology, people, and processes aligned in a way to enable "assured operations" in the presence of risks and adversaries. It involves the creation, operation, analysis, and testing of secure computer systems (including network and communication systems) as well as the study of how to employ operations, reasonable risk taking, and risk mitigations. The concept of "Cyber Sciences" refers to a broad collection of such programs, and disciplines under this umbrella often also include aspects of law, policy, human factors, ethics, risk management, and other topics directly related to the success of the activities and operations dependent on such systems, many times in the context of an adversary [6].

Our program is also very influenced by the Department of Defense and its perspective. *Joint Publication 3-12 (R) Cyberspace Operations* defines cyberspace as, "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" [7]. *Joint Publication 3-12 (R)* categorizes cyberspace operations (CO) as:

> Offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DODIN[1] based on their intent. OCO are CO intended to project power by the application of force in and through cyberspace. DCO are CO intended to defend DOD or other friendly cyberspace. DODIN operations are actions taken to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation [7].

Another effort we wish to highlight is the Military Academy CYBER Education Working Group which consists of members from United States Military Academy, United States Naval Academy, United States Air Force Academy, United States Coast Guard Academy, Naval Postgraduate School, Air Force Institute of Technology, US CYBER Command (USCC), and National Security Agency (NSA). The Military Academy CYBER Education Working Group was established in 2012 to develop a body of knowledge for undergraduate cyber education at the military academies. The working group believes that cyber education should include three levels: (1) what all officers should know, (2) what cyber leaders should know, and (3) what highly technical officers should know. The working group doesn't specifically define what cyber is, but it does lay out recommended curriculum guidelines for each of the three levels in the following nine areas [8].

1. Characteristics of the Cyberspace Domain
2. Cyberspace Risk Management
3. Cyberspace Operations, Planning, and Management
4. Cyber Attack
5. Cyber Defense
6. Authorities, Policies, and Law
7. Human Factors
8. Personal Responsibility and Ethics
9. Technology

There are many other education and scholarly efforts to define and describe cyber-related topics, curriculums, skills, and attributes of a professional. Both the IT2008 curricular guidelines [4] and the CS2013 curricular guidelines [9] include an Information Assurance and Security Knowledge Area in the respective bodies of knowledge. In 2011, a prescient paper from Brigham Young University provided a formidable literature review of cyber security work up to that time [10]. The paper also strongly advocated for increased emphasis on cyber security in IT education and presented recommendations that cyber security be viewed as multi-disciplinary in nature and that it be taught across the entire IT curriculum as opposed to just in security courses. This paper also highlighted the ongoing issue and importance of defining cyber when it stated that "there are some variations in the definition and scope of cyber-security that have been the cause of contention between authors" and spent a section illustrating those diverse viewpoints [10]. In 2012, an insightful paper describing the U.S. Naval Academy's first year cyber security course defined cyber as "the totality of the space in which new kinds of computer crime, terrorism, espionage, and warfare are taking place" [11]. In 2014 and 2015, *ACM Inroads* had issues that included impactful special sections on cyber security education [12, 13].

There have also been government and industry efforts to impact the cyber profession. These include the National Initiative for Cybersecurity Education (NICE) National Security Workforce Framework [14], the U.S. Department of Labor *Cybersecurity Competency Model* [15], and the U.S. Department of Energy's *Essential Body of Knowledge -- Competency and Functional Framework for Cyber Security Workforce Development* [16].

Influenced by all of the above sources, we "currently" define cyber by defining the Cyber Domain to be the following:

> *Cyber Domain*: A global ever evolving domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers – as well as people, organizations, and processes – which create a dimension of risks, adversaries, and opportunities.

Our working definition of the Cyber Domain includes almost verbatim the definition of cyberspace from *Joint Publication 3-12 (R)*, we added the words "ever evolving," with the following appended: "– as well as people, organizations, and processes – which create a dimension of risks, adversaries, and opportunities."

[1] DODIN: Department of Defense Information Networks

This extension is inspired by both the Cyber Education Project's definition of Cyber Sciences and by the description of cyber given in a speech at the United States Military Academy by Admiral Rogers (Commander, USCC and Director, NSA) in January of 2015. The extension makes explicit that the domain requires both people and processes to operate and to be relevant, and the inherent reliance of organizations on cyber. We then define our learning outcomes in terms of the Cyber Domain, such as "Explain the attributes, capabilities, risks, actors, implications, and interdisciplinary nature of the Cyber Domain."

This section's discussion of the definition of "cyber" only scratches the surface on the important topic of the meaning and connotation of the term. At this phase of its evolution, one of the important aspects of cyber is reaching convergence and consensus on what people mean when they use the term, which will lead to better unity of effort in evolving the profession.

3. A MULTI-LEVEL, MULTI-DISCIPLINE APPROACH

This section describes a multi-level, multi-discipline approach to cyber education that provides all educated individuals a level of cyber education appropriate for their role in society.

In this curricular model, cyber education includes technical and non-technical content across all levels. The levels include: general education content, giving all students exposure to the basics of cyber; disciplinary and interdisciplinary cyber electives, in areas like Political Science, Law, and Computing, providing opportunities to supplement one's education with cyber-related content; elective or embedded-in-a-major cyber-focused threads, providing the opportunity to specialize in cyber at a level less than a minor but more than a single course; cyber minor(s), covering both technical and non-technical knowledge areas; and technical and non-technical cyber-related majors that prepare graduates to succeed in the Cyber Domain. Our model does not currently include cyber major(s). We are, however, actively engaged in the Cyber Education Project's efforts to explore and develop "undergraduate curriculum guidelines and a case for accreditation for educational programs in the Cyber Sciences" [6]. Figure 1 illustrates the various levels of this approach and the following subsections describe how each level is instantiated at West Point.

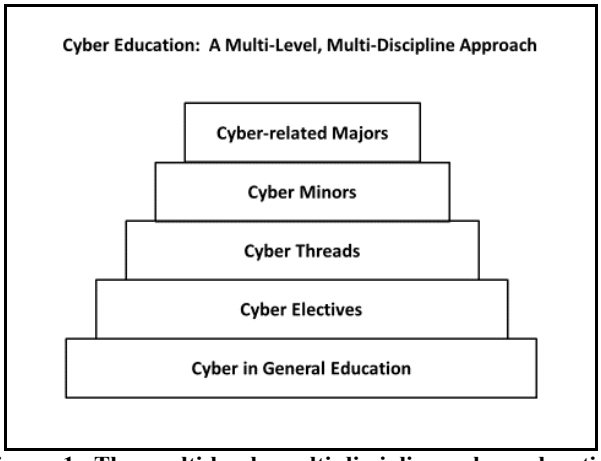

Figure 1. The multi-level, multi-discipline cyber education approach.

3.1 Cyber in General Education

Although compared with many other four-year institutions West Point has extremely stringent core education requirements in lieu of general education requirements, the premise of putting cyber into general education courses applies equally well at any college or university. Here we describe an approach that includes a required introductory information technology course, an intermediate-level information technology course required for all students not enrolled in a major that otherwise completes our cyber general education goals, and additional areas in the curriculum that expose all students to relevant cyber knowledge and attitudes in other disciplinary domains.

At West Point, all students are required to take an introductory information technology course. Three quarters of the course covers foundational computing and problem solving concepts necessary to function in the Cyber Domain, including about 20 lessons devoted to the fundamentals of programming and 10 lessons covering computing concepts such as hardware, networking, and common system and application software. Most of the remaining lessons in this course more directly address cyber including personal cyber security, tools such as encryption, digital signatures, and steganography, cyber warfare, the attributes of the cyber domain, cyber crime, cyber ethics, professionalism in a cyber environment, and intellectual property laws in cyberspace. It is our opinion that concepts and knowledge along these lines should be part of any general education information technology course.

Our institution has a number of computing and engineering majors that possess substantive cyber content. Any student who isn't majoring in one of these more technical majors also takes a second intermediate-level information technology course. This more advanced course covers information technology topics such as databases, web technologies, and digitization. It also devotes about a third of the course to networking, information assurance, and security -- culminating in three lessons during which all students conduct computer reconnaissance, defense, and attack within a virtual network environment. For the students in the computing and engineering majors that possess substantive cyber content, each major includes a set of experiences threaded throughout the major to collectively provide equivalent development to the intermediate information technology course described above.

As the cyber picture in the 21st Century emerges, we envision a taxonomy for cyber education across the entire spectrum of a curriculum, including many areas that are non-computing. In addition to the significant amount of cyber within our core information technology courses, cyber concepts (or materials directly supporting cyber concepts) are currently taught in small doses in such diverse general education classes as International Relations, Economics, Physics, Geography, Philosophy, and Law.

3.2 Cyber Electives

Cyber electives continue to emerge at West Point. In addition to the plethora of electives available within the Computer Science, Information Technology, and Electrical Engineering programs, West Point offers cyber focused courses to all students through special topics courses, interdisciplinary courses taught by faculty working together across departments, and introductory cyber courses that build on the required general education. Examples include a digital forensics course, an interdisciplinary cyber operations course covering operations, cyber law, and cyber policy that is co-taught by a Computing faculty member and an International Relations faculty member, an Applied Algebra with Cryptology course taught by the Mathematical Sciences Department, and a Cyber Ethics course that is taught by the Department of English and Philosophy.

3.3 Cyber Thread

In addition to the cyber content within our core education courses, all students not majoring in a program that otherwise accomplishes our problem solving and engineering requirements also take a three course engineering sequence, and one of the most popular options is the Cyber Engineering sequence. This sequence includes the following courses:

- IT300 – Programming Fundamentals
- IT350 – Network Engineering and Management
- CS482 – Cyber Security Engineering

By the end of this three course sequence, students have learned enough that they design, build, and defend a network during a multi-day capture the flag competition.

Additional cyber threads exist (or are being developed) in Computer Science, Information Technology, Electrical Engineering, Mathematics, and Network Science.

3.4 Cyber Minor

The Cyber Minor is five courses in addition to a student's other academic requirements. If a student has not taken the Cyber Engineering sequence elsewhere in their academic program, they must take it as three of their five courses. For students who have completed the Cyber Engineering sequence within their regular academic program, they take a mix of technical and non-technical courses from selections such as the following:

- CS483 – Digital Forensics
- EP395 – Cyber Ethics
- IT460 – Cyber Operations
- LW482 – National Security Law
- MA464 – Applied Algebra with Cryptology
- SS464 – Homeland Security
- SS465 – Terrorism: New Challenges
- SS486 – International Security Seminar
- XE492 – Disruptive Innovations

The principle audience for the Cyber Minor is non-computing majors, although it is also popular among our computing majors. Generally, the requirements of the minor are structured to promote an overall mix of computing and non-computing cyber courses. This minor supports students' desires to know and learn more about the Cyber Domain while simultaneously focusing on their chosen degree.

3.5 Cyber-related Majors

West Point offers technical, cyber-related majors in Computer Science (CS), Information Technology (IT), and Electrical Engineering (EE). These three programs provide superb preparation for service in the Cyber Domain. All three programs offer technical threads, or sequences of courses, that allow students to focus on their preferred sub-topics within their chosen major (e.g., CS's computer forensics, IT's networks and security, and EE's information assurance). The majors present cyber across the entire span of the curriculum and all include a culminating, nine-month capstone project, several of which are directly related to the Cyber Domain. Example capstones include developing cyber security education software, pinpointing a geographic location based on signals intelligence, network security projects, and engineering a network and then participating in the National Security Agency's Cyber Defense Exercise.

Additionally, many other Science, Mathematics, Engineering and non-technical majors, when matched with a Cyber Minor and the enrichment opportunities described in the next section, produce graduates prepared to contribute and lead within the Cyber Domain. Example majors include Defense and Strategic Studies, Geospatial Information Science, International Relations, Legal Studies, Mathematics, Operations Research, Political Science, and Systems Engineering.

4. ENRICHMENT OPPORTUNITIES

Enrichment opportunities are key to a culture and environment that inspires students to naturally apply the cyber curriculum. Student-driven independent study and undergraduate research experiences combined with a vibrant cyber extracurricular program creates tremendous synergy with the prescribed curriculum. This enhancement to the multi-level, multi-discipline model results in graduates who are truly formidable cyber professionals. West Point continues to expend considerable effort to develop, maintain, and grow enrichment opportunities. Although not the primary focus of this paper, we briefly describe here some of the current outside-the-classroom activities.

Clubs such as a student Competitive Cyber Team and a local chapter of an Association for Computing Machinery Security, Audit and Control (SIGSAC) Club provide students multiple local and national opportunities to experience cyber first hand. The competitive cyber team has tryouts each fall. It then regularly practices, and it participates in several national-level security competitions each year. The SIGSAC Club is open to all students and provides many hands-on security experiences in safe (air gapped) environments. These clubs also expose students to impressive guest speakers and even sponsor trips to ShmooCon and DEF CON - Black Hat.

Selected students are offered opportunities to attend SANS Institute [17], ISACA [18], and other education and training events and conferences. As example, this past spring break, 15 students attended six days of SANS training on the topics of security, hacking, and forensics.

Finally, most students interested in cyber also have one or more opportunities to participate in cyber summer internships. Organizations sponsoring these internships include IBM, Facebook, FBI, General Electric, NSA, Sandia Laboratories, Lincoln Laboratories, NATO's Cyber CERT, and many others. These internships provide unique opportunities to experience cyber in an operational, non-academic environment. Our relationships with these organizations also help identify possible collaborative projects as the students reach their nine-month senior capstone design project. These internships expose our students and their faculty to multiple facets of the Cyber Domain that might otherwise elude them.

Perhaps most importantly, throughout a student's undergraduate experience, there is a conscious effort to provide the culture, environment, and role models that grow them into cyber professionals and leaders who possess the character and competence our constituents demand.

Table 1 depicts a holistic summary of our cyber curriculum and enrichment opportunities. Table 1 represents an all-inclusive view of our multi-level, multi-discipline approach. We find that our efforts pay off for the students, who are in high demand among our cyber-focused constituents.

5. CONCLUSION

The principle contributions of this paper included (1) a discussion of the diverse challenges and viewpoints involved in defining the term cyber and (2) presentation of a multi-level, multi-discipline

approach to cyber education that addressed all educated individuals. We advocated seeking convergence and consensus among the many diverse participants in the rapidly evolving cyber education domain. Additionally, a paradigm was presented for how to conduct cyber education across multiple levels and multiple disciplines. We described a model of formally integrating cyber throughout an institution's entire curriculum, including within the required general education program, in offerings of cyber elective topics in multiple domains, in offerings of cyber threads, in a cyber minor, and finally in having major programs that provide the foundational knowledge, skills, and abilities needed to succeed in the 21st Century Cyber Domain. We also briefly highlighted the value that cyber extracurricular enrichment opportunities can provide to support and complement in-class instruction.

As the Cyber Domain continues to emerge and grow, we seek further debate, discussion, and increased involvement on the critical topic of cyber education. We hope our multi-level, multi-discipline educational approach has a positive impact on this effort.

Table 1. A holistic summary of the cyber in-class and enrichment opportunities our students experience.

Opportunity	All	Some	Few
Cyber in General Education	X		
Cyber Electives		X	
Cyber Threads		X	
Cyber Minor		X	
Cyber-related Majors			X
Cyber Independent Studies			X
Cyber Undergraduate Research			X
Competitive Cyber Team			X
SIGSAC Club		X	
SANS, ISACA, and other training			X
Cyber Summer Internships		X	
Culture and Role Models	X		

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense, or the United States Government.

6. REFERENCES

[1] The Colloquium for Information Systems Security Education (CISSE). http://www.cisse.info/. Accessed 25 May 2015.

[2] The National Initiative for Cybersecurity Education (NICE) Annual Conference and Expo. http://csrc.nist.gov/nice/. Accessed 25 May 2015.

[3] The Georgia Tech International Security Education Workshop. https://www.gtisc.gatech.edu/. Accessed 25 May 2015.

[4] Association for Computing Machinery and IEEE Computer Society. *Information Technology 2008 Curriculum Guidelines for Undergraduate Degree Programs in Information Technology*. November 2008. https://www.acm.org/education/curricula/. Accessed 25 May 2015.

[5] National Security Agency and the Department of Homeland Security National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD). https://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml. Accessed 25 May 2015.

[6] Cyber Education Project. http://cybereducationproject.org/. Accessed 25 May 2015.

[7] United States Department of Defense. *Joint Publication 3-12 (R) Cyberspace Operations (5 Feb 13)*. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf. Accessed 25 May 2015.

[8] Military Academy CYBER Education Working Group. *Draft Cyber Body of Knowledge*. http://computingportal.org/sites/default/files/CEWG%20-%20Draft%20Body%20of%20Knowledge.pdf. Accessed 25 May 2015.

[9] Association for Computing Machinery and IEEE Computer Society. *Computer Science Curricula 2013 Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*. December 2013. http://dl.acm.org/citation.cfm?id=2534860. Accessed 25 May 2015.

[10] Dale C. Rowe, Barry M. Lunt, and Joseph J. Ekstrom. "The Role of Cyber-Security in Information Technology Education." *Proceedings of the ACM Special Interest Group for Information Technology Education Conference*. October 2011.

[11] Christopher Brown et al. "Anatomy, Dissection, and Mechanics of an Introductory Cyber-Security Course's Curriculum at the United States Naval Academy." *Proceedings of the ACM Conference on Innovation and Technology in Computer Science Education*. July 2012.

[12] *ACM Inroads*. Volume 5, No. 1. March 2014.

[13] *ACM Inroads*. Volume 6, No. 2. June 2015.

[14] The National Initiative for Cybersecurity Education (NICE) Careers and Studies. *DRAFT National Cybersecurity Workforce Framework Version 2.0*. http://niccs.us-cert.gov/research/draft-national-cybersecurity-workforce-framework-version-20. Accessed 25 May 2015.

[15] U.S. Department of Labor. *Cybersecurity Competency Model*. http://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx. Accessed 25 May 2015.

[16] U.S. Department of Energy. *Essential Body of Knowledge – A Competency and Functional Framework for Cyber Security Workforce Development*. http://www.energy.gov/sites/prod/files/2014/04/f15/DOEEBK_1-2013Revision_NICEv01_SCRM_clean_v04.pdf. Accessed 25 May 2015.

[17] The SANS Institute. https://www.sans.org/. Accessed 25 May 2015.

[18] ISACA. https://www.isaca.org/. Accessed 25 May 2015.