3-2021

Creating a Multifarious Cyber Science Major

Raymond Blaine
United States Military Academy

Jean Blair
United States Military Academy

Christa Chewar
United States Military Academy

Rob Harrison
United States Military Academy

James J. Raftery
United States Military Academy

See next page for additional authors

Recommended Citation

Raymond W. Blaine, Jean R. S. Blair, Christa M. Chewar, Rob Harrison, James J. Raftery, Jr., and Edward Sobiesk. 2021. Creating a Multifarious Cyber Science Major. In Proceedings of the 52nd ACM Technical Symposium on Computer Science Education (SIGCSE '21), March 13–20, 2021, Virtual Event, USA. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3408877.3432462

Creating a Multifarious Cyber Science Major

Raymond W. Blaine
raymond.blaine@westpoint.edu
U.S. Military Academy
West Point, New York, US

Jean R. S. Blair
jean.blair@westpoint.edu
U.S. Military Academy
West Point, New York, US

Christa M. Chewar
christa.chewar@westpoint.edu
U.S. Military Academy
West Point, New York, US

Rob Harrison
rob.harrison@westpoint.edu
U.S. Military Academy
West Point, New York, US

James J. Raftery, Jr.
james.raftery@westpoint.edu
U.S. Military Academy
West Point, New York, US

Edward Sobiesk
edward.sobiesk@westpoint.edu
U.S. Military Academy
West Point, New York, US

ABSTRACT

Existing approaches to computing-based cyber undergraduate majors typically take one of two forms: a broad exploration of both technical and human aspects, or a deep technical exploration of a single discipline relevant to cybersecurity. This paper describes the creation of a third approach—a multifarious major, consistent with Cybersecurity Curricula 2017, the ABET Cybersecurity Program Criteria, and the National Security Agency Center for Academic Excellence—Cyber Operations criteria. Our novel curriculum relies on a 10-course common foundation extended by one of five possible concentrations, each of which is delivered through a disciplinary lens and specialized into a highly relevant computing interest area serving society's diverse cyber needs. The journey began years ago when we infused cybersecurity education throughout our programs, seeking to keep offerings and extracurricular activities relevant in society's increasingly complex relationship with cyberspace. This paper details the overarching design principles, decision-making process, benchmarking, and feedback elicitation activities. A surprising key step was merging several curricula proposals into a single hybrid option. The new major attracted a strong initial cohort, meeting our enrollment goals and exceeding our diversity goals. We provide several recommendations for any institution embarking on a process of designing a new cyber-named major.

CCS CONCEPTS

• **Applied computing** → *Education.*

KEYWORDS

cyber science, cyber-physical systems, network services, machine learning, cyber operations, cybersecurity, curriculum development

ACM Reference Format:
Raymond W. Blaine, Jean R. S. Blair, Christa M. Chewar, Rob Harrison, James J. Raftery, Jr., and Edward Sobiesk. 2021. Creating a Multifarious Cyber Science Major. In *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education (SIGCSE '21), March 13–20, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3408877.3432462

SIGCSE '21, March 13–20, 2021, Virtual Event, USA
2021. ACM ISBN 978-1-4503-8062-1/21/03.
https://doi.org/10.1145/3408877.3432462

1 INTRODUCTION

In early 2020, the graduating class of 2023 became the first freshmen to enroll in our new Cyber Science major. Most of them would be stunned to learn how long debate had raged among faculty at our institution, which ultimately concluded with the curriculum proposal that made their major selection possible. In fact, the majority of this first cohort of students was in elementary school when the debate began. In 2011, the faculty in our Department of Electrical Engineering and Computer Science (EECS) and our institutional leadership were already openly discussing the question of how best to address the emerging call to ensure adequate student exposure to security-related curricula from a technical perspective. Around that time, the word "cyber" also began to creep into our disciplines' lexicon; some faculty argued that we ought to be using that word more—in lectures, in course titles, even in names of academic programs—just to convey relevance. More traditionally-minded computer scientists and electrical engineers pushed-back, worried instead about chasing an industry-driven trend that soon would be regarded as passé in academe. Although we considered a trailblazing path that might have resulted in one of the first-offered, first-accredited cyber majors in the world, we instead opted for a more careful, methodical approach that built upon a strong understanding of the emerging discipline.

While this paper describes the curriculum initiative that culminated in the offering of a Cyber Science major, the deeper story is the transition in our thinking that allowed a full appreciation of the discipline as an academic area that will persist for many decades. A central aspect of this was appreciating the foundational knowledge, skills, and abilities that are useful educational preparation for workroles within the cyber workforce–many of which extend beyond the more narrow scope of cybersecurity. We sought to tease out the enduring concepts that will persist far beyond the transitory, short life-span of specific tools, policies, and even technologies. It was also critical to be able to describe this new discipline in a way that distinguished it from established majors that we offer, to include computer science (CS), electrical engineering (EE), and information technology (IT). Finally, we were eager to achieve best-possible understanding of perceptions among students from diverse backgrounds regarding the appeal of this new discipline, with the hope of broadening their representation in our student population.

Based on our deliberate research and curriculum development process, we believe that our insights will help inform a broader perspective on a cyber-focused program of study offered from a technical perspective. It was only after we found a suitable adjective–*multifarious*–to describe our program that we completely understood its uniqueness. We define this adjective here for the reader's convenience: **multifarious,** *having many kinds of parts or elements; of great variety; diverse; manifold*[14].

2 BACKGROUND CONTEXT

To fully appreciate the roots of our multifarious Cyber Science major, it is helpful to understand the context from which it evolved. A significant influence is the academic mindset at our institution, to include four important facets:

- a relatively large general education requirement that provides a broad, liberal arts foundation,
- an unspoken predilection for time-tested relevance over the immediate, fickle needs of the workforce,
- decades of faculty effort toward inspiring students reluctant to study technology, rather than solely the enthusiasts, and
- an understanding that our constituent graduate employers need graduates with skills broader than cybersecurity alone.

We explain why this mindset made the early adoption of a cybersecurity major undesirable several years ago, yet how these same forces eventually shaped our curriculum initiative. What came between was the tremendous efforts of the computing education community and accreditation bodies to describe cybersecurity curricula (which we discuss in Section 2.2) and the surge of demand for graduates in a new cyber workforce, both set against a backdrop of nearly constant world-changing events that underscored the importance of this new discipline.

2.1 Cyber Science Roots—but Early Rejection

Although serious discussion about cyber education began in 2011 among our EECS department faculty, this was just one step in an evolution that began decades earlier. Starting in the late 1990s, our faculty had been promoting both curricular and extracurricular initiatives focused on cyberspace.

Our forceful advocacy for Information Assurance led to a 2004 addition to our university's general education requirements—a junior-level information technology course that exposed all students to various technologies which allow data to be sensed, collected, transmitted, protected, and used for competitive advantage. Since this was a high-enrollment course, most of our faculty experienced the significant challenge of convincing students who major in non-technical fields to invest the intellectual effort necessary to understand these inherently technical topics. Additionally, we introduced an IT major in the mid-2000s to appeal to a larger and more diverse population than typically found in our traditional CS and EE programs. We also put great effort into developing curricula that reached the widest audiences by making our required freshman-level introductory computing course more accessible and creating inspirational summer workshops to introduce rising high school seniors to our undergraduate majors.

For decades, our department has also promoted extracurricular experiences in cyberspace by encouraging our students to compete fiercely in prominent cyber defense exercises and the earliest hacking competitions, as well as coordinating hundreds of summer internship opportunities each year that often exposed our undergraduates to cyber-related projects and workroles.

While these initiatives had the tremendous benefit of generating student enthusiasm for cybersecurity topics, by 2011 we were starting to notice some undesirable cultural effects.

- Select students would too often ignore or belittle the traditional and theoretical topics in the CS and IT major.
- A toxic, elitist "bro-grammer" hacker culture began to develop among student competitors, discouraging knowledge sharing and teamwork with new members (especially at the expense of increasing diversity).
- Computing courses that include a heavily applied, ever-evolving security focus were very difficult to maintain at a high-level of quality over time.
- The early surge of IT enrollments dwindled as a culture developed that incorrectly characterized the major as a fallback to CS without unique contributions to a multi-disciplinary team.
- A noticeable fissure between the computing and engineering efforts in the department began to emerge.

Little consensus existed at the time, even within the federal and commercial workforce, to define basic terminology and knowledge areas. High quality education materials, such as textbooks, tutorials, and lesson-support resources were also largely missing. For these reasons and others, creating a cyber-named degree was met with swift rejection; such an effort was thought to be a potential detraction from our established majors.

2.2 Continued Growth of Cyber Curricula

Despite our early decision against establishing a cyber-named major, for the years from 2013-2018, members of our faculty remained an active part of the cyber education research community, contributing to the compilation and promotion of the ACM/IEEE CS Joint Task Force on Computing Curricula CS2013[8], the Cyber Education Project[7], and creation of accreditation criteria for cybersecurity programs[1]. We kept tabs on, and contributed to, the growing body of educational research that began to achieve some cyber disciplinary identity, such as [2–7, 9, 12, 13, 15–19].

We were immensely influenced by the joint task force on cybersecurity education, supported by the computing professional societies ACM, IEEE-CS, AIS SIGSEC, and IFIP that defined cybersecurity as:

> 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 [13].

Their curriculum model, referred to as CSEC2017—shown in Figure 1, includes three components: a disciplinary lens—an underlying computing discipline; knowledge areas—organizing structure for

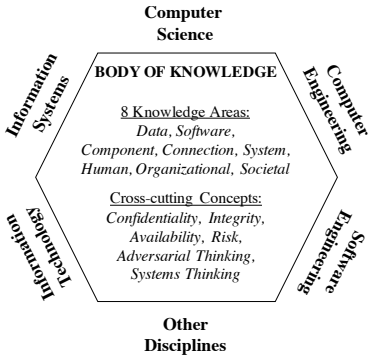

Figure 1: The CSEC2017[13] Curricular Framework.

curriculum content; and crosscutting concepts—connections across knowledge areas.

During this period, we watched as the post-graduation placement opportunities within the growing cyber workforce began to vastly increase for our graduates. Taking full advantage of our faculty's significant practitioner experience, as well as engagement and sabbatical programs, we were fortunate to have numerous faculty members serve within the national cyber workforce and reflect on the educational preparation of our graduates. Thus, we came to appreciate the nuances between the various workroles in the cyber workforce, depicted in Figure 2. Each of the four workroles (left side) in the figure require education covering topics in three broad knowledge areas (top): humans, hardware, and software. Areas of study (right side) are depicted in differing colors and correspond to the colored regions inside. Larger regions imply deeper coverage. For example, an adequate academic experience for a user (who is part of the cyber workforce) might be a general education that spans the three knowledge areas. The more specialized workroles, however, demand more depth in each of those knowledge areas, but in different and complementary ways. A developer with a cyber-physical systems focus will have the deepest coverage in some aspects of both hardware and software development, complemented with aspects of the human element.

Throughout the 2013-2018 time-frame, we also continued to create and refine new courses with a cyberspace-focus, available for elective credit in a wide variety of majors. The introduction of a Cybersecurity Minor became a very popular new offering, accessible by any major. Simultaneously, our department's EE faculty expanded coursework focused on robotics and controls topics. A few examples of new courses are detailed below.

Cyber Security Engineering - A senior-level course originally designed for CS and IT majors was redesigned to be accessible to non-engineering majors, providing a "capture the flag" network defense scenario as a culminating exercise.

Digital Forensics - A highly specialized elective for CS majors who have completed Operating Systems allows greater coverage of software reverse engineering and bytecode analysis.

Cyber Policy, Strategy and Operations - A required course for IT and an elective for International Relations majors is an interdisciplinary survey of current national cyber policy and strategy.

Cyber Ethics - A thought-provoking, writing-intensive elective is offered by our Department of English and Philosophy.

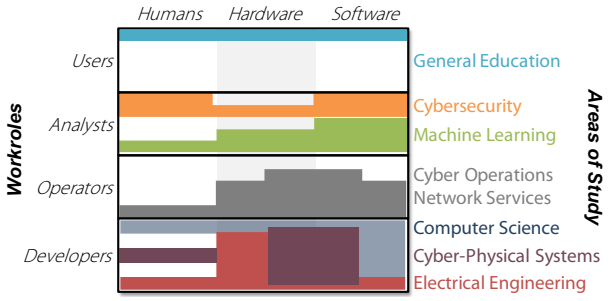

Figure 2: A Perspective on Desirable Levels of Education.

2.3 The Right Time Arrived

In late 2018, our new department head called for fresh consideration of offering an explicitly cyber-named major given our rich cyber-relevant offerings. As faculty investigated this question, a data point emerged the following summer, showing rising interest levels of high school seniors polled during our annual workshop and suggesting the time for a cyber-named major had arrived.

To get a sense of how other undergraduate schools developed cyber programs and increase our own faculty's buy-in for this new effort, during the summer of 2019, we benchmarked cyber majors at 11 other institutions, four of which were accredited under a "pilot test" for the ABET CAC's Cybersecurity Program Criteria. The benchmarks consist of two groups of institutions: the four programs accredited under ABET's pilot test (Towson, Southeast Missouri State, the US Air Force Academy, and the US Naval Academy) [11], and seven other programs accredited under ABET's general criteria for either the CAC or EAC or no accreditation at all at the time (Ferris State, Robert Morris, Central Florida, Northeastern, DePaul, Louisiana Technical, and Virginia Tech). The names of these programs varied substantially: Cybersecurity, Cyber Forensics and Information Security, Cyber Science, Cyber Operations, Computer Science with Computer Security Track, and Cyber Engineering. Collectively the bench-marked programs are characterized by:

(1) The wide range of programs approached cyber education from diverse CSEC2017 disciplinary lenses.
(2) Some programs relied heavily on deep mathematics as a foundation; others did not.
(3) Four institutions had earned the NSA CAE-CO (Cyber Operations) designation, while four earned the NSA/DHS CAE-CD (Cyber Defense) designation [20].
(4) At that time, four programs had earned ABET accreditation for the Cybersecurity program criteria or CAC General Criteria, while three programs had earned ABET accreditation under the EAC General Criteria or Computer Engineering.
(5) The programs varied widely in the college through which an institution offered the program, e.g., College of Arts and Science, College of Business, College of Engineering.
(6) Programs varied widely in prioritization of breadth versus depth in the discipline.

By 2019, we had achieved a shared vision of the discipline and its constituent workroles that allowed us to design our own cyber-named major, ensuring a high-quality educational experience and producing distinctly different outcomes in our graduates.

3 MAJOR CREATION PROCESS

Although our department leadership encouraged a rapid curriculum development process, there was little consensus among our faculty on how exactly to go about this. While there was general acknowledgment that creating a new cyber major would only be possible with the removal of our IT major, this caused significant angst: that we might end up losing enrollment of diverse students (to include student athletes, women, and racial minorities), or that a glitzy degree title might attract students to a less academically demanding program and away from well-established majors that might better meet their development needs. To address these concerns, committee efforts were taken to carefully articulate the broad overarching principles that should guide the curriculum development process and then develop and compare multiple fully viable options. Details of these efforts are provided below.

3.1 Broad Overarching Design Principles

We were able to find a productive starting point for the new major by explicitly stating several curriculum design goals. Goal statements that could not be agreed to by our senior-faculty did not survive the first cut. The new cyber-named major should:

- Prepare graduates to be lifelong learners in the cyber domain, regardless of their chosen career.
- Produce service-minded individuals who:
  - are user and enterprise-centric, enabling others to thrive,
  - flourish at creatively making solutions that meet organizational constraints,
  - are forward-thinking and, when appropriate, are likely to initiate actions that will have a long-term impact on policies and/or laws, and
  - embrace emerging technologies.
- Develop the multi-disciplinary skills necessary to work in teams with individuals from a broad range of disciplinary backgrounds; cultivate a unique set of skills relative to their teammates.
- Provide breadth of knowledge across appropriate related sub-disciplines.
- Provide depth in one or more area(s) of the discipline.
- Provide an enduring educational foundation, preparing graduates to succeed in graduate school.
- Be designed with ABET accreditation in mind.
- Be designed with NSA-CAE CO designation in mind.

3.2 Initial Options and Screening Criteria

Rather than just having a single faculty member design a specific new curriculum, the committee invited submissions from any interested faculty member. Some options were developed to address specific goal statements, while others represented the passionate feelings of its designer. The only rule that governed development options was that they must be possible within the constraints of our university's standard student course load. Options were presented to the committee by their designer, evaluated against screening criteria for possible elimination, and then scored against our agreed-upon decision criteria (shown in Table 1) based on group consensus. The screening criteria ensured all options would not negatively impact students currently enrolled in the IT major, conformed with the stated broad overarching principles, and included "cyber" in its name.

The most viable options are included here to show the variety of curriculum models considered.

Decision Criteria	How to Measure
Steady-state cost. Change in teaching/admin load. Assume 10% enrollment increase.	**Less is better** 0 by default; +/-1 per projected change in FTE
Transition cost. Number of new courses, changes to existing courses; measured as percent of contact time.	**Less is better** 0 by default; +/-1 for each new/retired course; +1 each major course-focus change
ABET. Meets ABET Curriculum Criteria	**More is better** 1 = yes; 0 = no
NSA/CAE-CO. Meets NSA/CAE-CO curriculum criteria; measure as overall change in relevant institutional coverage.	**More is better** 3 = all paths meet criteria; 2 = significant improvement, 1 = some improvement; 0 = no change
Network focus. Develops strong networking skills	**More is better** +1 per course w/ strong focus
Unique skills. Develops unique skills relative to other majors offered	**More is better** +1 per unique competency
Graduate school preparation. Admits options for high-quality technical graduate study	**More is better** 2 = multiple options; 1 = at least one option; 0 = no known option
Available. Implementation speed, based on projected year of first graduate	**More is better** 0 current freshmen class; +/- every year accelerated or delayed
Accessibility. Is broadly accessible to students of various math backgrounds and academic capability	**More is better** 0 by default; -1 each math beyond calculus; -x if course count = 18 + x; -1 each course w/ $>$ 2 prereq levels
Appeal. Appeals to a substantive number of institution's applicants	**More is better** % that agree or strongly agree on Likert scale responses
Student choice. Allows choice between deep technical or broad across technical, human, and organizational aspects	**More is better** 0 by default; 1 = one or two electives; 2 = choice of multi-course options (both deep and broad)
Institutional friction. Quantity and severity of obstacles to gaining curriculum approval	**Less is better** 0 by default; 1 = minimal; 2 = moderate; 3 = extensive

Table 1: Decision criteria.

Option 1—IT-Renamed. This IT-focused option would simply rename the existing IT major and make minimal changes necessary for accreditation as a cybersecurity program, as described in [10].

Option 2—IT-Evolved. This IT-focused option would be a true evolution of the IT major to more deeply address cybersecurity.

Option 3—CSEC2017 Inspired. Based on CSEC2017, this option would address the breadth of the cybersecurity discipline.

Option 4—Cyber-Physical Systems. This option would be a unique blend of depth components from both the CS and EE majors, providing a solid foundation for engineering secure control systems.

Option 5—NSA CAE-CO Focused. This option would explicitly address requirements that would allow student attainment of the NSA CAE-CO certification.

The results of the quantitative scoring (after weighting the decision criteria and normalizing the raw data) ranked Option 1 highest, which was disappointing after exploring other great ideas for more radical change. Our intuition was that IT-Renamed was not what we as a faculty thought was needed. Each of the other options had clear strengths highlighted by the decision criteria, but important weaknesses as well. While this process was wonderful for creating hope among skeptical faculty that viable ways forward existed, it left the committee frustrated with a desire to have them all!

3.3 Is a Hybrid Option Viable?

Realizing the importance of a multi-disciplinary approach to cyber as we reflected again on the diverse academic needs of the cyber workforce (see Figure 2), what started as a whimsical thought experiment soon turned into a serious endeavor. Through a course factoring process and very minor compromises, we created a hybrid option as a faithful composite of options 2-5. First came the identification of a 10-course foundation that was common to all options. The next level of factoring reflected a literal interpretation of the CSEC2017 disciplinary lenses concept and allowed student choice of four or five additional courses that would establish either an IT or CS/Computer Engineering background on which a concentration focus could be explored with a few more courses. Initially, we only had four concentrations, but quickly recognized the potential to add a fifth for a machine learning concentration as well.

We only gained confidence in the viability of the hybrid option after performing a detailed audit of topical exposure that would be received through all possible paths. This exercise prompted the decision to add two new courses: one on cyber algorithmics and another focusing on organizational security. Major redesign efforts would also be needed in a handful of courses, but this was a small cost for such a major improvement to our department's offerings. When we scored this new option with the decision criteria, it came out far better than Option 1.

4 A MULTIFARIOUS MAJOR

The structure of the Cyber Science major, depicted in final form by Figure 3, includes the 10 foundational courses (top left), the choice between two disciplinary lenses (IT in blue, moving right or CS/Computer Engineering in green, moving down), and the five concentrations. Although the complexity of the hybrid option worried some faculty, the vast majority regarded the hybrid option as true curriculum improvement. The five concentrations are described here:

Enrollment by Concentration	
Cybersecurity	15.6%
Network Services	6.7%
Cyber Operations	64.4%
Cyber-Physical Systems	6.7%
Machine Learning	6.7%

Table 2: Initial enrollment by concentration.

Cyber Science: Cybersecurity, a course of study that focuses on the interdisciplinary study of people, processes, and technology to assure operations in the face of cyberspace risks.

Cyber Science: Network Services, a course of study similar to a traditional IT major, but focused on building and securing the networks and services fundamental to operating in cyberspace.

Cyber Science: Cyber Operations, focusing on the low-level and technical skills that enable offensive and defensive cyberspace operations. This concentration most closely satisfies the requirements to earn a NSA/DHS CAE-CO certificate.

Cyber Science: Cyber-Physical Systems, providing a unique blend of depth in both hardware and software to understand networked, physical systems that are controlled by algorithms.

Cyber Science: Machine Learning, preparing graduates to gain insight using algorithmic tools that exploit large datasets and the Internet-of-Things (IoT).

An unintended (but most welcome) side effect of selecting the hybrid option brought together CS and EE courses and faculty which previously had no connections. It soon became clear that this complex curricula needed a name that would subsume the composite disciplinary specializations. *Cyber Science* provides an umbrella term that includes multiple academic perspectives (multifarious!) which transcend a more singular, highly-applied focus like security. Students are able to choose the disciplinary lens and concentration that best matches their interests, and their transcript can reflect this specialization.

Our new Cyber Science major was met with encouraging levels of student interest—more than doubling the previous years' IT enrollment—without overwhelming constrained teaching resources. Cyber Science attracted nearly equal enrollment to the CS major, which also attracted healthy enrollment. EE enrollment also maintained consistency compared to previous years. We were most encouraged to see the diversity of students that signed up for Cyber Science, including approximately one-third women and robust inclusion of underrepresented minorities. We were surprised to see that the Cyber Operations concentration attracted nearly two-thirds of the initial enrollment, although multiple students selected each concentration (Table 2). We look forward to observing changes in enrollment patterns over the next few years. To date, academic advisors have not encountered any novel challenges despite the complex structure of the major.

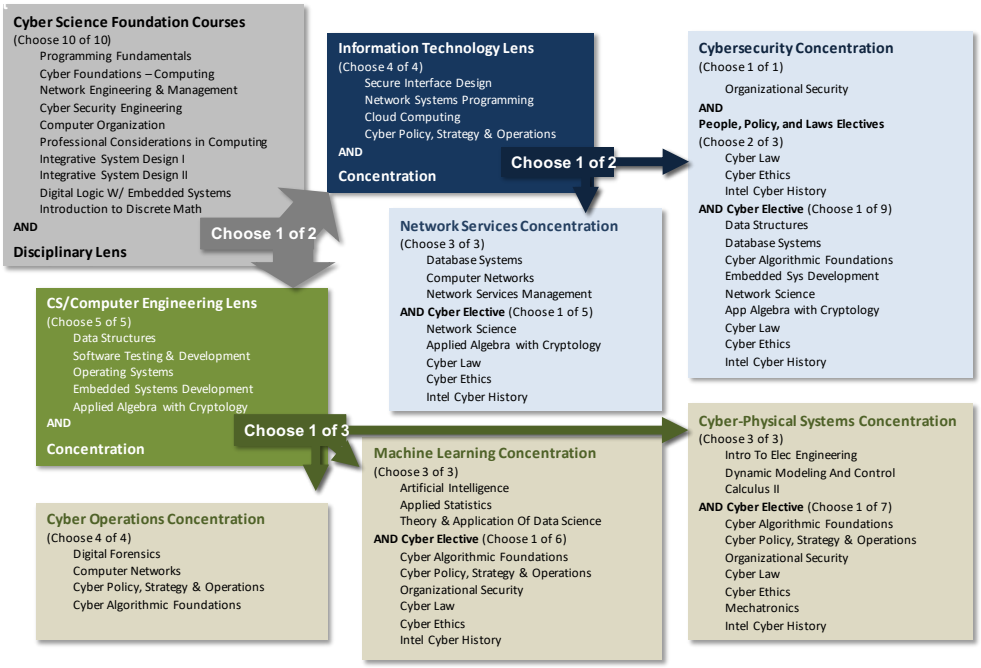

Figure 3: The Cyber Science Major: 10 foundation courses (top left), a disciplinary lens choice, and choice of concentration.

5 RECOMMENDATIONS AND INSIGHTS

Based on our experience creating a multifarious Cyber Science major, we offer a few recommendations that should be interesting to the community focused on computing education and other institutions considering adding a cyber-named major. At the very least, these ideas may prove interesting topics of debate that would allow a faculty to assess their readiness with offering a new cyber major.

- Take an incremental approach to developing cyber curricular content by progressively introducing electives to existing programs, such as CS, IT, EE, and even humanities and social science offerings, later connecting them with a few introductory courses that cover CSEC2017 topics.
- To create a multifarious cyber-named major, involve faculty with expertise across a spectrum of cyber-related disciplines who have the passion for multi-disciplinary collaboration. Understand that academic concerns within the broad "cyber umbrella" transcend the more narrow focus of cybersecurity.
- Identifying distinctive graduate competencies is very important early in the curriculum development process–what unique knowledge, skills, and abilities will graduates bring to a multi-disciplinary team better than any other major? We think one critical skill is risk analysis and management that incorporates an adversarial mindset.
- Be multifarious. Design a program that extends CSEC2017 to include multiple disciplinary lenses for broad appeal to diverse students who will likely have a variety of career goals. Extending the lenses with specialized concentrations can help add appeal and skill depth.
- Look for unique opportunities to leverage synergies between existing disciplines to open paths to new multi-disciplinary cyber concentrations, such as cyber-physical systems.
- Reflect on near-final curricular design to consider additional structure for emerging areas that might broaden student choice and allow faculty development.

Looking to the future, there are many undergraduate cyber majors now being offered that conform to the wonderful curricular guidelines which have appeared, such as CSEC2017, ABET's criteria for cyber programs, and the NSA-CAEs. However, as these communities generate new curricular guidelines, we advocate for consideration of how to produce technically-grounded graduates who are best prepared for an increasingly multi-disciplinary world.

An essential component of this is the broader adoption of foundational cyber coursework in general education requirements, spanning the knowledge areas defined by CSEC2017. There is great potential to attract broader diversity of students by establishing connections through traditional non-technical courses, such as international relations, law, ethics and philosophy, business, and even history. One should also anticipate the integration of emerging technologies such as machine learning, quantum, and 5G/IoT.

Finally, exemplars of Cyber Science student research/capstone project work results are needed to demonstrate the great diversity of research and analytical methods they have mastered, as well as the unique skills they bring to the table. As our students matriculate through the program, we hope to find venues and communities embracing cyber-focused research and educational best practices, helping to ensure Cyber Science majors and educators fully appreciate the impact of their multifarious disciplinary contributions.

ACKNOWLEDGMENTS

Tom Babbitt, Jon Bentley, Tanya Estes, Andy Hall, Alex Mentis, Roy Ragsdale, and Aaron St. Leger contributed significantly to the creation of the Cyber Science major at West Point. All participants in the 2019 EECS Senior Faculty Offsite added to our benchmark results and helped refine the design of the major. Numerous others helped by evolving our cyber-related programs over the course of a decade.

The views expressed in this paper 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.

REFERENCES

[1] ABET, Inc. 2019. Criteria for Accrediting Computing Programs, 2020–2021. https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2020-2021/ Accessed: August 27, 2020.

[2] Jean R. S. Blair, Christa M. Chewar, Rajendra K. Raj, and Edward Sobiesk. 2020. Infusing Principles and Practices for Secure Computing Throughout an Undergraduate Computer Science Curriculum. In *Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education* (Trondheim, Norway) *(ITiCSE '20)*. Association for Computing Machinery, New York, NY, USA, 82–88. https://doi.org/10.1145/3341525.3387426

[3] Jean R. S. Blair, Andrew O. Hall, and Edward Sobiesk. 2019. Educating Future Multidisciplinary Cybersecurity Teams. *Computer* 52, 3 (2019), 58–66. https://doi.org/10.1109/MC.2018.2884190

[4] Jean R. S. Blair, Andrew O. Hall, and Edward Sobiesk. 2020. Holistic Cyber Education. In *Cyber Security Education: Principles and Policies*, Greg Austin (Ed.). Routledge, New York, Chapter 10, 160–172.

[5] Diana L. Burley. 2014. Cybersecurity Education, Part 1. *ACM Inroads* 5, 1 (March 2014), 41. https://doi.org/10.1145/2568195.2568210

[6] Diana L. Burley. 2015. Cybersecurity Education, Part 2. *ACM Inroads* 6, 2 (May 2015), 58. https://doi.org/10.1145/2746407

[7] Cyber Education Project 2014. *About the CEP*. Cyber Education Project. https://cybereducationproject.org/ Accessed: August 27, 2020.

[8] Andrea Danyluk, Steve Roach, Elizabeth K. Hawthorne, Henry M. Walker, Ruth E. Anderson, and Christa M. Chewar. 2013. ACM/IEEE Computer Science 2013 Exemplar-Fest. In *Proceeding of the 44th ACM Technical Symposium on Computer Science Education* (Denver, Colorado, USA) *(SIGCSE '13)*. Association for Computing Machinery, New York, NY, USA, 285–286. https://doi.org/10.1145/2445196.2445284

[9] Joseph J. Ekstrom, Barry M. Lunt, Allen Parrish, Rajendra K. Raj, and Edward Sobiesk. 2017. Information Technology as a Cyber Science. In *Proceedings of the 37th SIGITE technical symposium on Information Technology education (SIGITE '17)*. ACM, New York, 84–89.

[10] Joseph J. Ekstrom, Barry M. Lunt, Allen Parrish, Rajendra K. Raj, and Edward Sobiesk. 2017. Information Technology as a Cyber Science. In *Proceedings of the 18th Annual Conference on Information Technology Education* (Rochester, New York, USA) *(SIGITE '17)*. Association for Computing Machinery, New York, NY, USA, 33–37. https://doi.org/10.1145/3125659.3125697

[11] David Gibson, Vijay Anand, Josh Dehlinger, Charles Dierbach, Tracy Emmersen, and Andrew Phillips. 2019. Accredited Undergraduate Cybersecurity Degrees: Four Approaches. *Computer Magazine* 52, 3 (March 2019), 38–47.

[12] Association for Computing Machinery (ACM) Joint Task Force on Computing Curricula and IEEE Computer Society. 2013. *Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*. Association for Computing Machinery, New York, NY, USA.

[13] Joint Task Force on Cybersecurity Education. 2017. *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. Technical Report. ACM, IEEE-CS, AIS SIGSEC, and IFIP WG 11.8. https://doi.org/10.1145/3184594

[14] Merriam-Webster. 2004. *Webster's New World College Dictionary* (fourth ed.). Collins Dictionary. https://www.collinsdictionary.com/us/dictionary/english/multifarious accessed August 25, 2020.

[15] Allen Parrish, John Impagliazzo, Rajendra K. Raj, Henrique Santos, Muhammad Rizwan Asghar, Audun Jøsang, Teresa Pereira, and Eliana Stavrou. 2018. Global Perspectives on Cybersecurity Education for 2030: A Case for a Meta-Discipline. In *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* (Larnaca, Cyprus) *(ITiCSE 2018 Companion)*. Association for Computing Machinery, New York, NY, USA, 36–54. https://doi.org/10.1145/3293881.3295778

[16] Mihaela Sabin, Svetlana Peltsverger, Cara Tang, and Barry M. Lunt. 2016. ACM/IEEE-CS Information Technology Curriculum 2017: A Status Update. In *Proceedings of the 17th Annual Conference on Information Technology Education* (Boston, Massachusetts, USA) *(SIGITE '16)*. Association for Computing Machinery, New York, NY, USA, 102–103. https://doi.org/10.1145/2978192.2978241

[17] Ann Sobel, Allen Parrish, and Rajendra K. Raj. 2019. Curricular Foundations for Cybersecurity. *Computer* 52, 3 (March 2019), 14–17. https://doi.org/10.1109/MC.2019.2898240

[18] Edward Sobiesk, Jean Blair, Gregory Conti, Michael Lanham, and Howard Taylor. 2015. Cyber Education: a multi-level, multi-discipline approach. In *Proceedings of the 16th Annual Conference on Information Technology Education (SIGITE '15)* (Chicago Illinois). ACM, ACM digital library, 43–47.

[19] Valdemar Svabensky, Jan Vykopal, and Pavel Celeda. 2020. What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences. In *SIGCSE '20: Proceedings of the 51st ACM Technical Symposium on Computer Science Education*. ACM, ACM digital library, 2–8. https://doi.org/10.1145/3328778.3366816

[20] US National Security Agency and the Department of Homeland Security. 2018. Centers of Academic Excellence in Cybersecurity. https://www.nsa.gov/resources/students-educators/centers-academic-excellence/ Accessed: April 02, 2018.