CYBERSECURITY AS A STANDALONE BACCALAUREATE DEGREE: ISSUES AND CHALLENGES

Allen Parrish (aparrish@research.msstate.edu)
Office of Research and Economic Development
Department of Computer Science and Engineering
Mississippi State University
Mississippi State, MS 39762
April 2018

Cybersecurity specialty programs are rapidly arising in numerous institutions and contexts. Frequently these programs are AS, MS, certificate or executive education programs – often taught in a non-traditional way (e.g., on-line) and/or by non-traditional (e.g., for profit) providers. In contrast, four-year baccalaureate programs have tended most frequently to augment traditional computing programs with cybersecurity content. Such programs continue to be, say, computer science programs – but with an increase in the amount of cybersecurity content. This approach is supported by, and in many cases the result of, the addition of significant cybersecurity content into all five of the longstanding ACM/IEEE-CS detailed curriculum volumes that contain recommendations for Computer Science, Information Systems, Information Technology, Computer Engineering, and Software Engineering. The recent integration of a cybersecurity requirement into the ABET Computing General Criteria is also a contributing factor toward the inclusion of cybersecurity content in existing computing programs. This "integration approach" takes advantage of the maturity of existing disciplines to anchor security concepts to mature disciplinary frameworks.

The various models described above for cybersecurity-focused programs are insufficient to meet the demand signal from industry for cybersecurity professionals over the next several years. As a result, institutions are beginning to develop standalone baccalaureate cybersecurity programs like more traditional majors in the academy (e.g., chemistry, physics, computer science, math, etc.). The recent publication of a sixth ACM/IEEE-CS detailed curriculum volume for cybersecurity called CSEC2017 supports the notion of standalone cybersecurity degrees, although contextualized by a "disciplinary lens" based on one of the traditional computing areas. ABET has also developed cybersecurity accreditation criteria for baccalaureate programs called "cybersecurity" or a similar name. The US Department of Education IPEDS data shows 93 US higher education institutions reporting cybersecurity degrees in 2016, with anecdotal observation and informal surveys at recent computing education conferences showing that standalone baccalaureate programs will grow rapidly. I call this approach the “standalone approach.”

The increase in standalone cybersecurity baccalaureate programs offers an opportunity to change the way that traditional universities approach teaching cybersecurity. The standalone approach offers traditional college students a highly attractive alternative to computer science and other computing programs. My recent experience with such a program (Cyber Operations) at the US Naval Academy is anecdotal evidence of rapidly increasing interest – from 22 majors in the current (2018) graduating class to 110 majors in this year’s freshman class. This type of growth could have a very positive impact in the large on the cybersecurity workforce over the next few years – where there are projected to be many unfilled positions.

While this increase could have a strong positive impact on the labor pipeline, there are still many issues and unanswered questions regarding cybersecurity as a baccalaureate educational program and/or as a first-class academic discipline within the academy. Some of these issues and unanswered questions are:

- CSEC2017 is a broadly defined document that is purported to cover all of cybersecurity. However, CSEC2017 is way too broad to be covered in four years. To limit its scope, CSEC2017 is shaped by a desired cognate computing discipline that functions as a disciplinary lens, thereby emphasizing some parts over others. The impact of the lens, however, has not yet been demonstrated – as it is dependent on examples that have not yet been developed. A demonstration of the feasibility for baccalaureate application of CSEC2017 (shaped by appropriate lenses) is still needed. Moreover, it is not clear how CSEC2017 supports the idea of a generic cybersecurity degree without a specific cognate computing discipline.
- Is there a useful nomenclature/taxonomy of different types of cybersecurity degrees? Currently, I am aware of cybersecurity programs in colleges and departments across the entire academy: Engineering, Computing, Technology, Criminal Justice, Law, Political Science and Psychology – just to name a few. Are there distinct names for programs in these various areas that could be canonized? How does these distinct areas relate to the CSEC2017 idea of a disciplinary lens? ABET’s view of cybersecurity is as a computing degree requiring certain computing-based outcomes (such as design, implementation and

analysis), but obviously many of these degree types are not computing degrees by this definition. Is there a rational approach to incorporating cybersecurity *writ large* into the academy?

- If cybersecurity is going to be its own degree program and/or discipline, what are the fundamentals of that discipline? Is it possible to teach the fundamentals of cybersecurity truly as conceptual fundamentals rather than as tool-based training and demonstrations? Does the level of sophistication required in cognate disciplines to understand those fundamentals make cybersecurity impractical as a baccalaureate program that can be completed in four or five years?
- How should academic institutions organize themselves to deliver baccalaureate cybersecurity programs? Are cybersecurity departments the best organizational model? Can interdisciplinary program delivery models work or are the constituent departments stuck in the worldviews of their respective disciplines? What are appropriate qualifications of faculty who deliver cybersecurity programs?

The list of questions can be made arbitrarily long. While there is no consensus that has emerged to address these questions, if baccalaureate cybersecurity degrees are going to emerge at scale within the mainstream comprehensive university with uniform expectations of quality, a common conceptual framework may be useful:

- Given the breadth of cybersecurity, perhaps it would be useful to formalize a "meta-discipline" that is orthogonal to *all* existing disciplines that serve as its primary cognate partner in various programs. While the name of the meta-discipline needs thought, more important than the actual name is the notion of "cybersecurity-in-the-large" (the meta-discipline that defines the universe of cybersecurity *writ large*) versus "cybersecurity-in-the-small" (which represents the use of the name "cybersecurity" for a specifically focused major). We have seen several examples of the use of "Cyber Science" and "Cyber Sciences" as the name for the meta-discipline (e.g., Augusta University's new *School of Computer and Cyber Sciences*) – while there are pluses and minuses to such a name, it does have the advantage that it is not frequently used in-the-small, and therefore it looks more like a meta-discipline (especially in plural form – Cyber Sciences).

- Academic institutions could then either consolidate different specific cyber degree programs under a "School of Cyber Sciences," using different names for individual degree programs that would hopefully start to converge on common program names – or the degree programs could emerge within different existing parts of the university based on the "cognate partner" disciplines. In the latter model, cyber-related computing programs would emerge alongside existing computing programs, cyber-related engineering programs would emerge alongside existing engineering programs, and cyber-related law and criminal justice programs would emerge alongside existing law and criminal justice programs, etc.

Standalone programs should then be developed with an awareness of the broader context of the "cyber sciences," and an awareness of whether consolidation across multiple "cyber sciences" is eventually desired. It would then be appropriate to consider whether there is a common set of fundamentals across the various programs, and whether courses and content could be shared. The alternative is the usual anarchy as different parts of the academy introduce redundancy and compete unproductively for students and resources.

Biography

Allen Parrish is Associate Vice President for Research and Professor of Computer Science and Engineering at Mississippi State University. Prior to his appointment at MSU, Dr. Parrish was Professor of Cyber Science and Chair of the Department of Cyber Science at The United States Naval Academy. Dr. Parrish previously served for 26 years on the faculty at The University of Alabama in a variety of roles, including Professor and Founding Director of the Center for Advanced Public Safety. Dr. Parrish served on the Joint Task Force that developed CSEC2017 and is currently co-chair of the Joint Task Force for *Computing Curricula 2020*, as well as co-editor of an upcoming special issue of *IEEE Computer* on foundations of cybersecurity education. Dr. Parrish also co-chaired the development of the recent major revision of the ABET computing accreditation criteria, including the new program criteria for cybersecurity. Dr. Parrish received a Ph.D. in computer and information science from The Ohio State University.