A Constructive Build-the-Flag Contest

Matt Bishop

Summary. We have many people who know how to compromise existing systems, and capture-the-flag contests are increasing this number. We have a great shortage of people who know how to design and build secure systems. A contest to build secure systems to meet specific goals – a "make-the-flag competition" — could help with this problem.

The non-security of existing systems is widely known. In computer security curricula and competitions, a common exercise is to have students find flaws in existing systems. In some cases, the organizers of competitions make their own systems (such as DefCon's Clemency system). The goal of these exercises and competitions (called "Capture-the-Flag" or "CTF" contests here) is to teach students how easily vulnerabilities can be exploited, by having them do the exploitation; or to demonstrate their skills in doing so.

A variant of these CTF competitions is to provide the contestants with an existing system that is known to have vulnerabilities. They are given some period of time, such as a month, to harden the system so that any vulnerabilities cannot be exploited, and all attempts to do so are recorded. The systems are then attacked by other teams or a "red team" and the contestants are given points for the attacks they have blocked. These "Protect-the-Flag" ("PTF") competitions are more constructive than the CTF ones because the emphasis is on securing a system, not breaching it.

Consider the ultimate goal of security. It is to create systems that satisfy a specific set of requirements. The CTF competition focuses on showing an existing system fails to do this. A PTF competition focuses on protecting an existing but fundamentally non-secure system to prevent it from violating a set of security requirements. But neither of these do what a "secure system" is to do: demonstrate to some desired level of assurance that a system meets a set of specific requirements, including security requirements.

This suggests an alternate competition. Why not have the contestants design and implement a system to meet specific requirements, including security requirements? This competition, a "Make-the-Flag" (MTF) competition, has the contestant teams work from the

ground up to design and build a secure system, rather than work from the top down to take a system apart. Such a competition would of necessity involve a special-purpose system because designing and implementing a general-purpose system from scratch would take too long. Participants would be contestants or competitors who design and implement the systems; evaluators who score the system; judges, who score the contest; and the competition managers, who design the competition and manage it.

Of most importance to such a competition is the degree of specifications given. In all cases, the competitors must be told the requirements to be met. But there are two primary issues from the point of view of the contest developers.

The competitors may simply be told that their system must meet the given requirements, leaving how they do that completely up to them. In this case, the competitors must document their system well enough so the evaluators, who have never seen it, can verify that the system meet the requirements. The advantage to this approach is it offers the contestants the maximum degree of freedom, while teaching them to document their interfaces and other external features of their system thoroughly enough for the evaluators to be able to use their system. The disadvantage is that each system will likely have a unique interface, which will create more work for the evaluators.

The second is to include a specification of the interface as part of the requirements. This constrains the competitors in how the system is used, but it is realistic in that output requirements are common. Further, it eases the burden on the evaluators because they will not have to learn a new interface for each system.

A third way is to specify the hardware as well as the interface and other requirements. This is appropriate if the goal of the contest requires special purpose hardware for an interface. The contest can specify some or all of the hardware to be used.

These constraints are the only limits to the imagination of the people running the contest.

The problem we face now is not that we lack people who know how to attack systems. Indeed, part of our problem is that we have too many of them! An MTF competition shifts the focus to creating secure systems, and we lack people who can do that. It also forces students to pull together everything they have learned in computer science classes — software engineering, robust programming, networking, security, and so forth — to build a system that will be tested thoroughly for vulnerabilities. It will also encourage academia to put more emphasis on teaching this art of construction.

With a suitable reward system for the competition, and if as well done as CTF competitions, this contest could increase the number of people who can build secure systems.

Cybersecurity Ethics Education: On "Future-Proofing" the Education We Provide

In this idea paper, I propose a kind of ethics education for cybersecurity that I believe is needed if we are to have any hope of "future-proofing" the education we provide. Cybersecurity education equips students to take profound action in the world and at the same time positions them to operate in a space in which the rules are often ill-defined. The field of cybersecurity is far from establishing codified standards of ethics and the few laws we do have in this area lag woefully behind the speed of technological innovation. We must recognize that we are educating the decision makers of tomorrow who will play a significant role in shaping the future of society. Amidst the rush to prepare a generation of cybersecurity professionals, this requires that we develop long term educational innovations that can prepare tomorrow's thought leaders for the unknown and uncertain futures before them.

Although it is encouraging that the NICE Cybersecurity Workforce Framework and the CAE Knowledge Units, two of the major curricular guidelines for cybersecurity, address ethics in cybersecurity, they both rely on a rule- and compliance-based approach to ethics education. The NICE Framework includes knowledge of ethical hacking principles and techniques as well as knowledge of national and international laws, regulation, policies and ethics as they relate to cybersecurity.[1] Similarly, included among the CAE Core Knowledge Units is: Policy, Legal, Ethics and Compliance. This knowledge unit intends "to provide students with an understanding of information assurance in context of the rules and guidelines that control them," by having students list and describe applicable laws and policies, which includes responsibilities for handling vulnerabilities.[2]

While knowledge of relevant laws and policies are an important place to begin, I believe that a rule- and compliance-based approach to ethics education is insufficient for cybersecurity. I briefly offer two reasons for this, here. First, because our laws cannot keep up with the speed of technological innovation. A preeminent example supporting this claim is the chief law we have for regulating cyberspace, the 1986 Computer Fraud and Abuse Act (CFAA), which, according to Josephinne Wolff's recent analysis of five cases, struggles to

[1] Newhouse, William, Stephanie Keith, Benjamin Scribner, and Greg Witte. "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework." *NIST Special Publication* 800 (2017): 181, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

[2] CAE Community, "Policy, Legal, Ethics and Compliance," Core Knowledge Units (2018). https://www.caecommunity.org/resources/ku-cards/ku/policy-legal-ethics-and-compliance.

> regulate a space where, fundamentally, some of the activities we want to encourage among the good guys—finding new vulnerabilities in computer systems, testing the security of software and devices—are largely indistinguishable from the activities that we want to discourage when undertaken by the bad guys.[3]

We are preparing students to operate in a realm that is not yet well contained by laws, standards, and norms. We need to recognize this by preparing students to not only have knowledge of yesterday's rules and laws, but to also be able to envision and establish the norms, rules, and policies of tomorrow.

Second, I draw on the educational philosophy of John Dewey in claiming that an ethics education of direct instruction in following the rules only amounts to something "in the degree to which pupils happen to be already animated by a sympathetic and dignified regard for the sentiments of others. Without such a regard, it has no more influence on character than information about the mountains of Asia."[4] A student's own inclinations and prior beliefs play a significant role in determining their ethical conduct. Cybersecurity ethics education must recognize this and find innovative ways to draw upon students' own ethical inclinations. Dewey continues, maintaining that within a democratic society, to attempt to get reliable results through an ethics education of direct instruction is "to rely upon sentimental magic."[5] There is an irony here in that ostensively, we are endeavoring to develop a cybersecurity workforce in order to uphold our democratic society. Yet, in the case of cybersecurity ethics education, I suggest that we not only need to educate *for* democracy, but *through* it as well.

I conclude by proposing an alternative approach to cybersecurity ethics education that involves creating intentional space for engaging in a cumulative and ongoing process of ethical inquiry. In addition to imparting knowledge of relevant laws and ethical principles and practices, there is a need to cultivate wide-ranging capacities, skills, and dispositions that will enable cybersecurity professionals to utilize, reflect upon, and revise this knowledge-base throughout their careers. The aim of this alternative approach is to foster a kind of ethical culture that can endure in the face of uncertainty and ever-emerging potentialities.

---

[3] Wolff, Josephine Wolff, "The Hacking Law that Can't Hack It," *Slate* (2016), http://www.slate.com/articles/technology/future_tense/2016/09/the_computer_fraud_and_abuse_act_turns_30_years_old.html.

[4] John Dewey, *Democracy and Education*, New York: The Free Press (1916), 354.

[5] Ibid.

Jane Blanken-Webb is a Postdoctoral Research Associate at the Information Trust Institute at the University of Illinois at Urbana-Champaign, where she is taking the lead as co-principal investigator on a grant funded initiative, Ethical Thinking in Cyber Space (EThiCS), supported by the National Security Agency. The main aim of this grant is to develop and teach a cybersecurity ethics curriculum, which was piloted during the Spring semester of 2018. She holds a PhD specializing in Philosophy of Education from the University of Illinois at Urbana-Champaign and her work has been published widely in the field of education. In addition to extensive teaching experience at the university level, she has four years of experience teaching in K-12 environments. Jane and has been working in cybersecurity education since the Fall of 2016 and is closely involved with the Illinois Cyber Security Scholars Program, an NSF funded Scholarship for Service program.

SEVEN OVERLAPPING THESES ON CYBER-SECURITY EDUCATION

Scott Borg
Director and Chief Economist
U.S. Cyber Consequences Unit
scott.borg@usccu.us

The majority of the leading figures in real-world cyber security did not become the acknowledged masters of the field *despite* their unconventional and diverse academic backgrounds; they became the acknowledged masters *because* of their unconventional and diverse backgrounds. Entering the field of cyber security before there were regular university programs or even courses in the subject was actually an advantage. The current formalization of cyber-security training is in danger of actively *preventing* people from developing many of the skills and abilities that the field most needs. What's more, many of the proposals for improving cyber-security education would only make things worse.

The following seven theses are all essentially an elaboration of this point. They are based on many years of intensive, practical experience in cyber security, including in-depth, on-site investigations of nearly all the critical infrastructure industries. There wasn't room to describe the relevant experiences in this short paper. Most people with extensive practical experience in cyber security, however, will be able to think of many anecdotes that would support these seven theses.

Obviously, we need formal cyber-security training. We need far more practioners than could ever be produced or find their way into the field without regular academic programs. But we need to be sure that those programs are preserving at least some of the features that made many of the pioneering people in the field so adept and so innovative. We need to be sure we

are preparing people not just for entry level jobs, but for future leadership roles. We especially need to be sure that we are not doing things in our training programs that put our graduates at a disadvantage when it come to dealing with highly creative adversaries.

Thesis One: An over-emphasis on STEM training is often making students *less* equipped to do cyber security well. The subject matter of natural science, engineering, and math, can be predicted by extrapolating from past cases. As Einstein famously said, nature is subtle, but it is not malicious. The uncertainties in natural science can usually be modeled by normal distributions. The subject matter of cyber security is not like that. Cyber attacks, their practical consequences, and the ways they can be foiled cannot be predicted by extrapolating from past cases. Cyber-security practitioners regularly need to deal with phenomena that are not just subtle, but malicious and cunningly so. The uncertainties in the field can hardly ever be accurately modeled as normal distributions. The often dazzling creativity of cyber attackers needs to be met with equally dazzling creativity on the part of defenders. When systems are under attack, defensive actions often need to be taken based on an intuitive assessment of what is going on, with no time for a comprehensive, carefully reasoned analysis, testing, or verification. Yet at the same time, the field is so open-ended, there is no objective way to put a limit on the facts that need to be taken into account. The whole mindset of natural science, engineering, and math is therefore profoundly wrong for doing cyber security.

Thesis Two: The information assurance triad of availability, confidentiality, and integrity, which still dominates cyber-security education, is obsolete as the goal for cyber security. This is because these categories describe features of information systems and cause defenders to focus on their own technology, rather than on potential attackers. The goal of cyber security should be to reduce risk, defined as annualized expected loss. The way to do this is usually to increase attacker costs. This means that the focus, even at a very basic, practical level, should be on stopping the things that attackers need to do in order to make their attacks pay off. Cyber security practitioners, guided by the information assurance triad, can rarely describe with any accuracy more than one or two components of what they are trying to

prevent. Many of the most notorious cyber-security failures over the last several years can be traced to this failure in understanding.

Thesis Three: The *majority* of the topics cyber-security professionals most need to master in order to assess and reduce cyber risk are *not* covered in the curricula of most university cyber-security programs. This is partly because they are not included in the $(ISC)^2$ Common Body of Knowledge used for the CISSP exam, the NIST Cybersecurity Framework, or the other documents regarded by academics as defining the field. As a result, most cyber-security education focuses overwhelmingly on a narrow technical portion of the Vulnerability factor in the cyber-security risk equation. It largely ignores the other two factors in the risk equation: Consequence and Threat. When cyber-security programs pretend to address these other factors, they usually define them in a way that reduces them to aspects of Vulnerability. Despite the fact that economic factors drive almost everything that happens in cyber security, most cyber-security programs omit economics altogether. Even the specializations in cyber-security education are focused the wrong subjects. If cyber security is going to reduce risk, it needs to tailor its practices to the different economic and safety requirements of different industries. Yet cyber-security specializations are rarely organized by industry. Instead, the usual specializations regularly separate issues that, in practice, need to be handled together and by the same person. The NICE Framework, for example, puts many tasks into different work roles and different specialty areas that should never be performed by different people. Meanwhile, this same NICE Framework fails to distinguish between the very different cyber-security requirements of industries as distinct as railways, electronic manufacturing, healthcare, and financial services. At both a basic and an advanced specialist level, expecting cyber-security practitioners to protect industry systems without any genuine understanding of what those systems actually do, technically and economically, is a very bad educational strategy.

Thesis Four: The qualification hurdles designed to make sure that cyber-security professionals cannot get accredited without the types of expertise deemed most essential are effectively *excluding* the kinds of skills and expertise that are *really* most essential. Cyber security does not need practitioners who will faithfully do exactly what they were taught in

school nearly as much as it needs people who can tackle a subject without being told what to do. It does not need people who can remember exactly what they were taught nearly as much as it needs people who can continually re-think things, and who can move across different disciplines so casually that they are barely aware of doing so. Before there were university departments in computer engineering, programmers were typically recruited from language departments, philosophy departments, linguistics departments, and even music departments. The broader liberal arts background associated with those fields of study was often more valuable for their later work than any specific training they received in matters relating to computers.

Thesis Five: The effort to make the study of computers and programming academically respectable, by describing it as a "science," rather than as a field of engineering, and by emphasizing mathematics, especially the mathematics of analog physics, has caused adverse effects on cyber-security education that urgently need to be corrected. Hardly any of the mathematics computer engineering students are required to learn is of any practical use in practical programming, let alone cyber security. This means that the math requirements in computer engineering and cyber-security programs severely limit the available talent pool without delivering any compensating benefits. Worse, treating computer engineering as though it were a science to be pursued for science's sake results in graduates who design programs and systems that are too fragile for the real world. It is as though engineers were being taught to design bridges "for bridge's sake," without ever having to worry about things like traffic, winds, earth tremors, metal fatigue, temperature changes, and future uses. Companies often have to train "computer science" graduates from our best universities for an additional year-and-a-half to two years before they can use them for anything important. Even then, these graduates tend to retain work habits that are not conducive to things like secure programming.

Thesis Six: Where cyber security is concerned, cultural diversity is not a laudable social goal, but a *functional* necessity, and, even though most educational programs for cyber-security education pretend to encourage this diversity, they actually go to great lengths to eliminate it. One of the ways educational programs do this is by assuming that the correct answer to

almost every problem or test question will be same for every student. Real-world cyber security, however, depends on people seeing things differently, especially seeing things other people have missed, not only different ways of accomplishing the same things, but different things that could be accomplished. Cyber-security training should be encouraging and rewarding students who can come up with a *different* answer than anyone else. This is the opposite of current practice.

Thesis Seven: The technical jargon currently used in the profession and in many cyber-security courses is an obstacle to good cyber-security education. This is not primarily because of the barriers it puts between cyber-security professionals and the general public, but because it is riddled with fallacious assumptions, obsolete distinctions, category confusions, and usages inconsistent with better established disciplines. The terms used to describe cyber attacks, for example, do not follow any consistent principle. Some terms refer to propagation mechanisms, some to hiding places, some to activation times, some to attacker goals, some to technical effects, some to business effects, and so on, through at least sixteen principles of classification. The definitions cyber-security authorities, such as NIST, give for basic business and financial terms, such as "asset" and "risk," are often simply wrong. What's more, students tend to learn the technical terms, instead of the underlying concepts, and then get even the technical terms wrong. Despite these problems, most cyber-security programs, instead of making stringent efforts to avoid the jargon, pride themselves on teaching it. This has the further effect of making most cyber-security graduates incapable of defending their budgets when they are talking with senior business executives.

Scott Borg is Director and Chief Economist of the U.S. Cyber Consequences Unit, an independent, nonprofit research institute that investigates the strategic and economic consequences of cyber attacks. He is the leading authority on the economics of cyber security as well as a number of technical topics. He has been the principal proponent of a quantitative, risk-based approach to cyber security for nearly twenty years and is responsible for many of the concepts that are currently used to understand the effects of cyber attacks in business contexts. He is author of The ISA Guidelines for Securing the Electronic Supply Chain, the most comprehensive reference document for protecting electronics manufacturing. Along with John Bumgarner, he is co-author of the new US-CCU Cyber-Security Matrix, a complete survey of genuinely useful cyber defense measures, more than a thousand items long, organized according to the attacker activities they are designed to prevent. His other technical contributions have included pioneering work on the techniques for hiding and finding malware and new methods for analyzing it. Partly because of the way he has been able to employ economic models, his record for anticipating new developments in cyber security since 2002 is probably unequaled. He was able to predict Stuxnet, for example, its exact target, and exactly how it would reach and damage that target, fourteen months before it as found. He has been quoted in most of the world's leading news publications, comments for NBC, CNN, the BBC, NPR and other broadcast media, served on the Commission on Cybersecurity for the 44th Presidency, and has lectured at Harvard, Columbia, Berlin (Freie), and other leading universities. His current research is on the implications of cyber security for international relations.

New Approaches to Cybersecurity Education (NACE) Workshop
Topic: Making Socio-Technical Cybersecurity a Part of Educational Preparation
Chris Bronk and Wm. Arthur Conklin
University of Houston

Summary

While cybersecurity was once a small niche area, primarily, but not entirely contained in computer science and engineering, it is increasingly viewed as a significant societal problem. Getting "hacked" is a relatable experience to millions of Americans in personal or professional venues. But finding remedy or protection is far harder than being compromised by cyberattack. For this reason, we propose effort on connecting to disciplines in developing fundamental learning injects for cybersecurity that align with other forms of professional responsibility and ethics.

The Problem: Cybersecurity Outside the Cybersecurity "Priesthood"

Cybersecurity has become a fundamental component of the socio-technical environment where an enormous amount of work takes place. Professional activity in all manner of endeavor and enterprise is dependent upon a technological infrastructure that remains inherently insecure. Thus far, the primary response to our societal cybersecurity problem has been cybersecurity chiefly as a technical design objective; something to be engineered into a tool, a product, or a process. This focus on "build to deploy" efforts has resolved some issues but falls short of comprehensive remedy. Effective cybersecurity over the long-term requires greater breadth and wider penetration of cybersecurity behaviors across the entire range of activities enabled by information and computing technologies.

While we work to expand the professional cybersecurity workforce, there is an enormous unresolved question regarding our current efforts: *How do we integrate cybersecurity behaviors into the education programs for business, law, social sciences, medicine, and other areas?* The understanding of technology, its promise and limitations, as well as the responsibilities in employing it, requires the inclusion of cybersecurity know-how into a wide range of disciplines.

For example, consider the field of social work, an area of specialization that employs almost 700,000 people in the United States and will add 100,000 additional professionals by 2026.[*] Social workers observe client confidentiality, maintain records protected by multiple regulatory regimes, and increasingly employ digital tools as enablers for productivity. The question we want to answer for it is: How does social work curriculum need to incorporate cybersecurity into professional preparation? This is a question in need of application *to many fields*.

Cybersecurity for Everybody?

When we start approaching how disciplines should incorporate cybersecurity into decision-making, professional responsibility, and leadership, there is obvious pushback on simply

exporting general cybersecurity knowledge from computer science and engineering. Professionals in myriad fields need to know what is relevant to them – starting with regulatory items that may be detrimental to certification or continued practice in a given field – but accepting the need for practical professional preparation on cybersecurity will require new modes of identifying, encapsulating, and delivering relevant critical knowledge. Expanding cybersecurity education and training efforts to a wider audience should include presenting relevant material in many majors and professional degree programs: business (including MBAs); law and social science; psychology; science; medicine; and engineering among others.

One answer on cybersecurity outside of traditional areas in academia has been to leave the problem to employers. This often translates to online annual training that likely has little impact on cybersecurity awareness and behavior.[†] Critical thinking on cybersecurity in preparation and lifelong learning for non-cybersecurity professionals is desperately needed, but rarely found inside most undergraduate disciplines or higher levels of education. Consider Symantec's lead healthcare technical architect's statement from just last year, who said of medicine, "[W]ith the exception of a few 'doctor-turned-geek' type of characters, I [have] never interacted with a doctor on cybersecurity – meaning those doctors whose main role is delivering care and who have not shifted gears into the IT or regulatory space."[‡]

What Needs Doing

There is an unmet need in understanding what and how much security knowledge is needed by professionals as their careers become increasingly influenced or shaped by information and computing technology. Unfortunately, most have little expertise in how to employ them responsibly with regard to cybersecurity. Even in computing disciplines, there has been considerable debate in how much cybersecurity thinking need be horned into undergraduate and graduate degree programs.

Where we need to advance cybersecurity is in engaging with other fields – business, law, medicine, and many others – to create meaningful professional preparation that can be built upon as cybersecurity evolves. This will mean engaging with disciplines across the university. The objective is not to make people in all disciplines cybersecurity experts, but rather deliver targeted awareness to issues that are within the context of their responsibilities. For instance, social engineering and phishing education is needed by all who use email. But understanding how email works is far less important than knowing how actions and behaviors are manipulated by others in the medium. The need is in incorporating cybersecurity behaviors or logics into daily work.

Expansion of cybersecurity elements into other disciplines curricula needs to be context aware, and user context behavioral based elements should address the following areas of interest:

- What skills and knowledge should people in any respective field have, and how should that be acquired?

- What are proper ways to address the mix of education methods, industry practice, and government needs over a lifetime of work?
- What elements are discipline specific and what may be generalized across many areas of professional activity?

An Education Agenda

Academia has long offered "physics for poets" courses in the sciences that explain to non-physicists' concepts of the discipline that may be helpful to know. While requiring that all students take an introductory cybersecurity course would be folly, we do know that some cybersecurity knowledge is a necessity for doctors, lawyers, program managers, civil engineers, social workers, retail managers, schoolteachers, and many, many other professionals. They need to know how to responsibly employ computing technology with regard to cybersecurity in the conduct of their professions.

What needs to occur is determining what knowledge regarding cybersecurity can be imparted within the context of the recipient's professional preparation and career path. We are not suggesting that all students become cybersecurity experts, passing the *Security+* exam or being able to speak intelligently on the Diffie-Hellman key exchange, but rather they learn what's needed through targeted curricula, preferably in courses that already exist. No doubt, skilled experts will be needed to assist the workforce in reinforcing organizational cybersecurity capacity, but more work needs to be done on security behaviors for professionals employing systems that may be attacked via cyber means.

The engagement needed is between cybersecurity programs and the other areas of education and professional preparation undertaken in colleges and universities. The task at hand is to engage with other academic programs on incorporating cybersecurity knowledge and behavior with appropriate, tailored content by discipline in the context of professional responsibility.

---

[*] "Social Workers." Occupational Outlook Handbook. Bureau of Labor Statistics, Washington, DC, available at: https://www.bls.gov/ooh/community-and-social-service/social-workers.htm.

[†] Bada, M; Sasse, A; (2014) *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* Global Cyber Security Capacity Centre, University of Oxford: Oxford, UK.

[‡] Wirth, Axel. "The Doctor Is In." *Biomedical instrumentation & technology* 51, no. 6 (2017): 514-517.

Cybersecurity automation and security

Susan G. Campbell and Petra Bradley, University of Maryland

The roles of future cyber professionals

The future of cybersecurity will be automated. Like less skilled personnel in other industries, less skilled cyber personnel are already being replaced by automated systems. Deep learning systems and other forms of artificial intelligence are being used for intrusion detection and network monitoring tasks. Straightforward tasks in other domains, such as secure programming, can be implemented using complicated but deterministic rules. Unlike humans, automated systems do not suffer negative effects from extended vigilance and do not accidentally omit procedural steps to create security holes. The current shortage of qualified cyber personnel should increase motivation to develop automated systems to fill holes in organizations' security postures that would otherwise have been filled by people.

Personnel who understand cybersecurity will still be required, because human decision-makers are needed to specify and build these systems, operate them, audit their operation, check them for security flaws, and provide them with training data. Cyber jobs of the future will encompass these areas rather than more routine actions, and people who are engaged in cyber work must also anticipate human and organizational behavior to mitigate human-generated security concerns. The roles of personnel in cyber will not necessarily change from the roles listed in the National Initiative for Cybersecurity Education (NICE) Cyber Security Workforce framework, but the way people do those jobs will change.

Future cyber education topics to support those roles

Security personnel will be required regardless of the level of automation that is achieved, but those personnel might focus their efforts on supervising automated processes and making decisions, rather than performing routine monitoring or defense.

Understanding human and organizational behavior

Future cyber personnel will need to understand which problems can be solved using technological means and which problems are due to the fact that organizations are made up of humans whose main priority is not generally security. Curricula need to increase cybersecurity

students' understanding of humans and sociotechnical systems (made up of people and technology), not just the technology.

Designing and evaluating automation

Other fields, as well as cyber, are building automated systems to accomplish tasks that do not need to be performed by humans to be successful. For example, goods that were once assembled by humans are now often assembled by machines, with human supervisors who ensure that the machines are working properly and who are equipped to trouble-shoot the systems when necessary. Cyber systems should gather best practices from other fields. Students who are planning to build systems should learn information security and networking concepts along with the appropriate kinds of automation (rule-based, machine learning based, or hybrid).

In addition to being able to build automated systems, organizations need personnel who are capable of evaluating whether automated systems are working properly and who can troubleshoot problems when necessary (or, at minimum, identify problems correctly so they can request the right kind of assistance). Generally, this requires understanding the systems and how they are meant to interact when they are working properly.

Operating systems and providing training data

Automated systems can reduce the number of personnel in certain roles within cyber, but any organization should have some way of evaluating whether their systems are working appropriately. This can be ascertained by inspection and monitoring of processes, or by challenging the system (e.g., conducting a "red team" exercise). In machine learning based systems, training data that are appropriately labeled and tagged can greatly accelerate the process of building and evaluating effective systems.

Operators may not need the skills to design automation, but they should be able to execute human-machine teaming tasks and identify malfunctions. Students who are planning to operate systems should have an understanding of the underlying mechanisms, but do not necessarily need to be able to build systems.

Securing the security software

The people who are most skilled at building automated systems may not be those who best understand security. Therefore, cybersecurity curricula should include a track for "pure" security, which would include evaluating automated systems as well as advancing the science of security.

Future-proofing cyber education

The realm of cyber is ever-evolving, and the types of threats to cybersecurity are likewise a changing landscape. Constant change presents a unique challenge; unlike topic areas in which our understanding of the basic truths has been constant for decades (or much longer), cybersecurity risks can change over a very short period. Deliberate human actions like denial and deception also co-evolve with defensive actions. One way to prevent curricula from "going stale" is to focus on basic understanding of human motivation and behavior. Although the actions and mitigations occur in a technological context, they are carried out by human actors whose actions can only be observed by their digital fingerprints. Understanding how people might exploit capabilities of new technology will help cybersecurity professionals to anticipate and understand the behavior they see on the systems they protect.

Author bios

Susan G. Campbell is an Assistant Research Scientist at the University of Maryland Center for Advanced Study of Language (CASL) and a Lecturer at the University of Maryland College of Information Studies (iSchool). Her current research focuses on determining and measuring the cognitive abilities required for different tasks within the cyber workforce. In addition to teaching a human-centered cyber course, she works on curriculum development for cyber across programs within the iSchool.

Petra Bradley (not attending) is an Associate Research Scientist at the University of Maryland Center for Advanced Study of Language (CASL). She is a cognitive psychologist interested in human learning and memory, decision making, and human-machine teaming. Her current projects focus on human trust of recommender systems and detecting insider threat. She has worked extensively with language and intelligence analysts to determine how they use information systems and what types of automated assistance can best benefit them in their work.

A new approach for Bachelor degree in Cybersecurity

Agnes Chan
Northeastern University

Introduction.

With the rise in demand for cybersecurity professionals, comes along a proliferation of training programs. These programs range from online training to traditional degrees, from certification to master degrees, all with the goal of producing qualified cybersecurity workforce within a short period. Unfortunately, with all the programs available to students, the gap between supply and demand in cybersecurity workers remains large. More troublesome is the feedback from potential information technology (IT) employers stating that the product of these programs is underqualified. In the 2015 survey report on Cybersecurity Job Market[1], published by Burning Glass Technology, a workforce study company in Cambridge, it was found that 37% of IT employers indicated that fewer than 25% of the graduates are qualified. This leads us to ask questions such as "What is missing in these programs?", "Are we providing the correct training at the right level?", or is it that in our haste of mass producing cybersecurity workers, we are skimming over the fundamental knowledge of the field? This white paper will discuss the weakness of current practices, and propose a new direction in training cybersecurity professionals.

Cybersecurity and Healthcare Professions.

Cybersecurity concerns the protection of computer systems and networks. It builds on the fundamental knowledge of computer science, such as coding, operating system and network. These topics should be taught with similar depth as expected in computer science. However, it differs from computer science in that it concerns the proper functioning of its protected entities, even when they are under attack, whereas computer science concerns the use of computers to achieve efficient computation and engineering designs. The concerns of the two professions are different, the goals and approaches of the programs should be different. Currently, most of the cybersecurity programs follow the methodologies of IT or computer science education, with modification in requirements by adding essential, non-technical knowledge such as cyber law

[1] ISACA State of Cybersecurity 2017: Current Trends in Workforce Development

and human interaction. One other significant modification is the requirement of laboratory exercises. While laboratory exercise in a course provides hands-on experience in learning a focused cybersecurity concept, it does not provide graduates with a holistic view of the problem or vulnerability itself.

On the other hand, while the technical training expected in cybersecurity and healthcare are vastly different, the objective of being able to detect and protect their clients are similar in both disciplines. Both disciplines require fundamental concepts, upon which their disciplines are built. Nurses require basic understanding of biology and chemistry, while cybersecurity workers require fundamental comprehension of coding, systems and networks. Nurses need to know how to communicate with patients, how to look out for suspicious decease, how to provide simple treatment plans, and know when to notify doctors. These skills are taught in courses such as nursing practices and, nursing care for children or adult patients. A cybersecurity professional may not need to communicate with users often, but he needs to be able to detect possible vulnerabilities, to discuss his findings clearly and succinctly with his cybersecurity teammates, and to explore a possible solution to mitigate losses. Current programs do not provide courses within the curriculum to teach cybersecurity students this needed skill, it is left to the students to pick up the skill set through post graduate work experience or other venues. To remedy this shortcoming of the curriculum, we propose the introduction of practicum courses in the last 2 years of their study. These practicum courses allow students to observe and to learn how professionals work as a team to solve problems; they may even learn to participate in decision making through professional mentorship.

Collaboration: Government, Industry and Academia.

Similar to Nursing programs, cybersecurity programs will not succeed without the collaboration from government and industry. In general, academia lacks the opportunity and facility to provide on field training to cybersecurity students. Government and industry are asked to take students on site, mentor them, show them how decisions are made and how one person's behavior affects the entire system. Opportunities for students to observe and to learn are crucial for the success in the education of a cybersecurity professional. In addition, these practicum courses can serve as work experience required by IT managers.

Cybersecurity is also getting more challenging every day, especially with the introduction of new technology and its ensuing applications. One such example is the Internet of Things (IoT). The communication complexity, together with the intricacies of the technology and network infrastructure, have posted new security and reliability challenges to cybersecurity professionals. As new technologies are introduced, the attack surface grows, so does the variation of attacks. It is difficult for a cybersecurity professional to familiarize himself with all the new technologies. These technologies have to be taught and transferred from government and industry experts to security professionals. In addition, with current shortage of qualified cybersecurity educators, government and industry can help narrowing the gap by allowing their employees to teach part-time in academia.

In short, government needs to create programs that fund industry/government professionals to partake in the teaching of cybersecurity. Industry needs to provide expertise and mentorship in training students. It is only through these collaborations that cybersecurity professionals can be well prepared to face the challenges, now and in the future.

Other Mechanisms to Strengthen Cybersecurity Education.

Other strategies that can strengthen the training of cybersecurity professionals include

- *Textbooks*. Textbooks provide a venue to define cyber security taxonomy uniformly. Furthermore, textbooks provide a certain standard of depth in each topic area.
- *Conferences*. Papers accepted or presented by security conferences should include tutorial on new industry technology and the security issues anticipated. Small group discussions on cybersecurity experiences, such as "A problem I encountered and how I handled it", should be encouraged and arranged in conference meetings. Students, especially the MS students, often attribute their learning from peers. The small group discussion is to facilitate peer learning experience.

The cybersecurity community has been debating for the last decade on what knowledge units are needed to be included in the education program. This debate needs to continue to ensure that cybersecurity professionals possess the needed knowledge. But transfer of knowledge is a relatively easy problem to solve. The teaching of professional behavior and experiences require more thought. We are proposing a new paradigm in educating cybersecurity professionals based on how they are expected to perform as a professional upon graduation.

Biography.

Professor Chan received her PhD in mathematics and joined the Northeastern University faculty in 1977. She is currently the Executive Director of Information Assurance and Cybersecurity. Her research focuses on cryptography and communication security. She works on fast, efficient mutual authentication algorithms for small mobile devices. More recently, she focuses on cybersecurity workforce. Professor Chan holds two patents on stream ciphers. She has published widely in IEEE conferences and journals, as well as in Crypto and Eurocrypt. Her research has been funded by NSA, NSF, DARPA and telecommunication industries. She was awarded the Distinguished Educator Award presented at CISSE in 2016.

Professor Chan led the effort in establishing an interdisciplinary research Institute of Information Assurance at Northeastern University. She is the PI for Center of Academic Excellence in Cyber Defense, Research and Cyber Operations. She designed and launched the interdisciplinary programs in cybersecurityat at Northeastern University: MS in 2005, PhD in 2010 and BS in Cyber Security in 2017. Professor Chan has been active in promoting women in sciences, in particular, she has participated as an invited speaker at NSA's "Women in Mathematics" and "Alumni Mathematicians" at Smith College.

I intend to share my ideas from an information science perspective to address the question that has perplexed cybersecurity researchers and educators: "How do we get more US citizens—and a more diverse population —into cybersecurity in meaningful ways?"

The smart innovations ranging from wearable devices to smart homes to cars to medical devices have become part of our daily life and continue to shape our behavior in the foreseeable future. According to 2018 Global Megatrends in Cybersecurity by Ponemon Institute, 82% of IT practitioners predicted a data breach from unsecured Internet of Things (IoT) devices is very likely to occur in the subsequent years. However, a recent cyber-security knowledge survey by Pew Research Center reported most Americans had limited cyber-security knowledge, which implies that those with smart devices connected to the Internet are at higher risks of cybersecurity threats. While most Americans have limited knowledge about cyber-security concepts (like strong passwords and risks of public WiFi network), most of them are unfamiliar with the key technical cyber-security concepts, such as botnet, VPN, and two-factor authentication (Olmstead and Smith, 2017). This reveals the fact that there is an urgent need to increase the cyber-security knowledge level of general public in the United States.

Extending Existing Stop-Think-Connect Model to a Complementary Education Model for the Public: Learn-Think-Change

"Leaning without thinking leads to confusion; thinking without learning ends in danger." ~ Confucius

In 2010, President Obama designated October as National Cybersecurity Awareness Month. The Department of Homeland Security (DHS) has initiated the national campaign and promoted partnerships between public and private sectors using the hashtag #cyberaware. Apart from that, a cybersecurity awareness program, entitled Stop-Think-Connect from DHS, has been adopted as a cybersecurity education model for community colleges (Fernandez et al., 2016). Inspired by this model, I suggest considering how learning and behavioral change theories/models can contribute to creating a complementary education model of cybersecurity literacy, namely Learn-Think-Change, for the general public.

(1) Learning Cyber-Security Knowledge and Public Opinion of Cyber-Security Awareness on Social Media

Many scholars have been investigating the professional knowledge trends in cyber-security research based on scientific research publications. However, few efforts have been put into mining user-generated content relevant to cybersecurity knowledge exchange on social media platforms. It would be meaningful to monitor the informal knowledge and resources shared through the hashtag networks in social media-enabled electronic networks of practice (eNoPs). eNoPs refers to geographically dispersed virtual communities with members who may never meet each other but share the same professional interests and publicly exchange information, advice or resources online. Social media enables eNoPs to informally exchange knowledge across boundaries in a timely manner (Beck, Pahlke, & Seebach, 2014). Taking the healthcare field as an example, Healthcare Hashtag Project is an open platform for connecting healthcare stakeholders (i.e., patients, caregivers, advocates, doctors and other providers) to timely information on Twitter. Hashtag networks link social media enabled eNoPs among professionals with diverse backgrounds to a variety of information resources, including questions and answers, news, hyperlinks, videos, images, and so on. I think it would be helpful to have one similar initiative, Cybersecurity Hashtag Project, for connecting cybersecurity stakeholders and communities through hashtag networks to organically create a substantial knowledge base. Such an initiative has the potential to engage and influence both cybersecurity curriculum across disciplines as well as life-long continuing education for the public.

(2) Thinking about Cybersecurity Risks and Risk Information Seeking

Cybersecurity behavior is always a choice. People can choose how they respond and react to cybersecurity challenges. What cybersecurity behaviors and choices will serve people best depends on their cybersecurity risk perceptions and how they view and cope with cybersecurity risks. Human information behavior could serve as a bridge to understand how people seek, process, and share cybersecurity risk information to bridge their information and knowledge gap. Integrating the concept of risk communication from the field of communication and information behavior from information science, the risk information seeking and processing (RISP) model (Dunwoody and Griffin, 2015) appears to be an appropriate framework to discuss the factors influencing how people seek and process risk information to bridge their knowledge gap. It is worth noting that information insufficiency and informational subjective norm are the significant predictors that drive people's risk information seeking through different information channels. Though the RISP model was originally developed to examine motivations behind information

seeking and processing behaviors on mass media, the recent studies have shifted the focus to social media. Therefore, cybersecurity professionals could use this model to rethink their role in educating the public and influencing other professionals about seeking and acquiring cybersecurity risk information. Leveraging the perceived social influence from social media could be a meaningful way to motivate the public's desire to be informed pertaining to cybersecurity risks. As a result, risk information seeking plays an essential role in motivating people to make corresponding changes when facing cybersecurity threats, thus leading to an informed understanding of cybersecurity risks.

(3) Changing Cybersecurity Information Behavior by Choice Architecture Design (Digital Nudge of Secure Online Behavior)

Cybersecurity incidents will change the ways in which the public responds to and communicates about cybersecurity risks. Raising the awareness and knowledge level of cyber-security is the first step to trigger the cybersecurity behavioral change. Various approaches can contribute to intervention design of cybersecurity awareness and literacy. The successful experience of motivating health behavior change using choice architecture may be replicated in the field of cybersecurity. From the perspective of behavioral economics, Thaler and Sunstein (2008) proposed the notion of choice architecture and defined it as the presentation of choices that nudge user decisions. Since choice architecture aims to affect behavior change without forcing people to accept but informing them of potential choices, it considers impact evaluations of informative presentations. In the digital world, the concept of digital nudge has been proposed to provide "a sort of compass to help individuals navigate a world of choices" (Schüll, 2016, p. 303). Similar to the IRS tax map built on semantic integration and topic maps, a cybersecurity map combining different knowledge mapping tools (e.g., mind maps, concept maps, and topic maps) could be developed. Such a map can assist users in searching and navigating cyber-security and privacy concepts by providing decision aids for their tasks relevant to changing the security and privacy settings of their smart devices.

Summary

Social influence through social media is one of the characteristics that we could leverage to change public perception and human information behavior about cybersecurity risks. Information

professionals can help design interventions using choice architecture to address users' information needs. This could mean designing effective information architecture for websites and mobile applications or providing an integrated knowledge mapping tool to facilitate learning and conveying cybersecurity concepts. In this way, users can learn where to find more cybersecurity information and locate their needed resources in a timely manner.

Author's Bio Sketch

Hsia-Ching Chang is an assistant professor in the Department of Information Science, College of Information at the University of North Texas. She is affiliated with the Center for Information and Cyber Security (CICS) at University of North Texas. She received her PhD and MS in information science from the University at Albany, State University of New York as well as her MA in public policy from the National Taipei University in Taiwan. Her research interests concentrate on cybersecurity, data analytics, social media, knowledge mapping, scientometrics, information architecture, and information interaction. She got the Cloud Security Alliance's CCSK (Certificate of Cloud Security Knowledge) certified, the first IT certification for secure cloud computing. She has been teaching the graduate-level course, Information and Cybersecurity, since 2015. She is the co-editor of the new book "Analytics and Knowledge Management" in Data Analytics Applications Series published by CRC Press, Taylor & Francis Group. She is currently co-editing a book entitled "Cybersecurity for Information Professionals" to be published by Libraries Unlimited, ABC-CLIO in 2019.

References

Beck, R., Pahlke, I., & Seebach, C. (2014). Knowledge exchange and symbolic action in social media-enabled electronic networks of practice: a multilevel perspective on knowledge seekers and contributors. *MIS Quarterly*, 38(4), pp. 1245-1270.

Dunwoody, S., and Griffin, R. J. (2015). Risk information seeking and processing model. In H. Cho, T. Reimer & K. A. McComas (Eds.), *SAGE Handbook of Risk Communication* (pp. 102-118). Thousand Oaks, CA: SAGE Publications.

Fernandez, B. R., Garcia, C. A., Capriles, J. R., Ford, W. & Mooney, C. (2016). Building Bridges: From NSF I-Corps to Community Colleges – Cybersecurity for All. *National Cybersecurity Institute Journal*, 3(2), 11-23.

Olmstead, K., & Smith, A. (2017). Americans and cybersecurity, *Pew Research Center*. Schüll, N. D. (2016). Data for life: Wearable technology and the design of self-care. *BioSocieties*, 11(3), 317-333.

Thaler, R. H., & Sunstein, C. R. (1999). *Nudge: Improving decisions about health, wealth, and happiness*. New Haven, CT: Yales University Press.

Resources to Meet Cybersecurity Education Demands

By

Balakrishnan Dasarathy, PhD
Professor and Program Chair, University of Maryland University College, Adelphi, MD
Email: Balakrishnan.Dasarathy@UMUC.edu

The mission of the University of Maryland University College (UMUC) is to improve the lives of adult learners by operating as Maryland's open university, serving working adults, military service-members, their families, and veterans across the United States, and around the world. UMUC serves over 80,000 students worldwide and is one of the largest distance-learning institutions in the world. We have eight different cybersecurity and related degree programs at the undergraduate and graduate levels with specializations in software security, network security, cybersecurity technology, policy and management, digital forensics and information assurance, and about 11,000 students are currently enrolled in these programs. To increase access to quality higher education in cybersecurity at affordable cost (at UMUC and elsewhere), it is imperative that we develop several resources nationally. Nationally-developed resources not only amortize the cost over several institutions, they also prescribe and enforce certain minimum standards. The resources we need fall into the following categories (The need for many of these resources exists in other disciplines as well, but the need is more acute in our field.):

- (Hands-on) Laboratory exercises
- Environments for laboratory exercises
- Content
- Assessment materials

Laboratory Exercises: This is one area, as a field, we have made a good bit of progress. I am particularly aware of three programs funded by NSF, all of high quality. SEED at the University of Syracuse is a comprehensive one with laboratory exercises in network, web, software, system and mobile security, and cryptography. The Cyber4All exercises at Towson University focus on secure coding. The third one, a recent one, from the Florida Center for Cybersecurity includes exercises on incident response, penetration testing and malware analysis. All these three projects do have content support, but the content is tied to their laboratory exercises. UMUC will be using several of these laboratory exercises in a new program on Cyber Operations. To meet our cyber

workforce needs, it is imperative that NSF and other agencies continue to support this type of laboratory development work and transitioning the output to institutions nationwide.

Environments for Laboratory Exercises: Many universities need a laboratory environment with 24x7 support. Currently, in spite of advances in cloud computing and virtualization technologies, having a reliable computing environment for student teaching, and sandbox for research and experimentation cannot be taken for granted. Emulab and environments based on Emulab such as the DeterLab are better at supporting experimental research than instructional exercises by a large number of students. Several states (see, for example, Virginia Cyber Range, Baltimore Cyber Range) now offer cyber ranges for their citizens to practice their cybersecurity skills, but they are in preliminary stages of development. Students, in general, require a lot of hand-holding and assistance with trouble-shooting. Students in digital forensics also require access to a local, physical laboratory, as certain segments of computer science, telecommunication & networking students experimenting new concepts in operating systems, virtualization and cloud computing.

Content: I believe this is next frontier in higher education. As we know, textbooks are expensive and often students need to buy more than one textbook for a course. Fields like ours are also changing rapidly, and as such, textbooks become outdated within a few years after their release. An online version of a textbook is generally cheaper and supports revisions more easily than the corresponding hardcopy of the textbook. However, online textbooks, controlled by DRM software, have many restrictions such as short time of usage (often till the end of a specific semester), limited amount of printing, and restrictions on the number of devices; moreover, they are hosted on proprietary platforms. UMUC has had successful experience going "bookless" since 2015/2016, as noted in the one of the 2018 College Jeopardy Championship tournament episodes! With the assistance of subject matter experts, I have experience in developing content for seven courses in information assurance/cybersecurity over a two year period in areas that include network security, intrusion detection, digital forensics, cryptography, cyberlaw and privacy, and software assurance. My fear is that no single institution will able to keep up with content development and updating all on its own. Apart from the government supplied resources, specifically from NIST, there are very few "open resources." For a resource to be truly open, it should meet these 5 R's: (1) retain (make and own a copy of the resource), (2) reuse (use the

resource in many places), (3) revise (adapt/modify), (4) remix (combine the resource with other resources), and (5) redistribute (share the resource). With truly open educational resources that are self-contained, an instructor can easily tailor the content for a session or an entire course. Our community and sponsors should be encouraging high quality content development for degree programs at various levels. The National CyberWatch Center' Digital Press and EBooks, funded by NSF, is a good start here. The center also develops laboratory exercises and curricula, but the focus of the center currently is on community colleges and associate degree programs. MOOCs are a good development here as well, but, by and large, the content from MOOC courses have Intellectual Property restrictions. Moreover, content from a MOOC course might be tied to a specific platform and may not be easily portable and tailorable.

There are two competing requirements faced by higher education in content development today. One is the use of multimedia for enhanced learning experience. The other is in meeting the requirements of the Rehabilitation Act (1973) and Americans with Disabilities Act (1990, amended 2008). The key concept behind these acts is equal opportunity. A resolution agreement with the US Department of Education establishes that students with disabilities must be: "able to obtain the information as fully, equally, and independently as a person without a disability." At the minimum, in the short run, UMUC is committed to providing meaningful text alternatives for any non-text content. Technologies are available today (see, for instance, Office 365: Accessible by design) to create content that can be accessed without barriers as well for creating content by those who are challenged in some ways. Expanding access is not only the right thing but also the smart thing to do in meeting our cyber workforce needs!

Assessment Materials: To produce cybersecurity knowledge workers rapidly, our cybersecurity programs need to be more "open." We should not be demanding credentials (e.g., B.S. in Computer Science with 3.0 GPA); we should only be requiring that specific competencies be met. We need tailorable tests/assessments for verifying competencies. A good model to follow here is that of CYBRScore. The CYBRScore Skills Assessment is mapped to the NIST-NICE framework and employs hands-on scenarios to test competencies for a specific work role. For example, their Cyber Defense Analyst assessment consists of assessments for competencies in protocol analysis, intrusion detection, incident handling, and vulnerability analysis. This CYBRScore assessment technology is, however, proprietary. We need open solutions!

The Future of Security and Privacy Education:
Incorporating Cybersecurity Law and Policy into Cybersecurity Curricula

Paula S. deWitte, J.D., Ph.D., P.E.
Assistant Director, Texas A&M Cybersecurity Center and
Associate Professor of Practice, Computer Science and Engineering Department,
College of Engineering, Texas A&M University
Paula.dewitte@tamu.edu

What new approaches are required in educating the next generation cybersecurity workforce? (1) We cannot educate and train the large numbers of cybersecurity workers required in the United States. The question becomes: *How do we increase the efficacy of those we do educate and train?* (2) We have relative smaller numbers of women and other underrepresented groups in cybersecurity: Similarly, the question becomes: *How do we increase opportunities?*

The Issues: It is unarguable that the evolution of law and policy lags technology development. Both poorly anticipate what *may* occur; rather, society implements new laws and policies in reaction to events. Before the disclosures by Facebook and Cambridge Analytica, most analysts did not expect additional privacy regulations in the United States now being considered. Another issue is a current case before the Supreme Court of the United States (SCOTUS), Carpenter v United States.[1] The long standing legal precedent is that law enforcement does not require a Fourth Amendment Search Warrant to obtain data shared with a third party such as phone logs (i.e., numbers called, time called, call duration, and locations of the parties) with a vendor (i.e., the mobile phone service provider). The SCOTUS decision, due early summer 2018, may require such search warrants based on arguments that the pervasiveness of technology such as smartphones has fundamentally changed the power of technology to be more invasive in areas that individuals have a "reasonable expectation of privacy." Both issues, although seemingly incongruent, are concerned with privacy and protecting individuals when sharing data, either through "apps" or the government. These issues require cybersecurity workers to be cognizant when new legal and policy rules apply.

[1] https://www.oyez.org/cases/2017/16-402

Nor is this confined to domestic law and policy. Cyberworkers need to be cognizant of evolving privacy frameworks such as the General Data Protection Regulation (GDPR) with, among other issues, extra-territorial jurisdiction, broadly defined personal data of "data subjects," and the recognition that many non-EU countries are implementing GDPR (e.g., Singapore, Mexico, Canada).

Students studying cybersecurity today will be the front-line for protection, detection, and response to cyber attacks. They will make decisions within constrained time periods; yet, they are being educated without substantial knowledge of either American or international law and policy. These cyberworkers will not have the luxury of contacting legal counsel for advice because of the sheer volume of decisions and the need for rapid action. What is required is academic curricula devoted to cybersecurity law and policy to develop students' capabilities to analyze and confidently apply emerging laws and policies without constant reference to legal advice.

Such courses are often mis-labeled as "soft skills" and treated as an after-thought rather than an integrated component of cybersecurity curricula necessary to support technical decision-making. Educating front-line protectors, defenders, and responders through tailored course content and pedogeological processes improve the efficacy of cybersecurity workers. This is a better approach than educating more cyber savvy attorneys. [Good luck with that!] This is misguided. It creates yet another legal specialty within the already burdensome, time-consuming legal process, and does nothing to address cyberworkers time-dependent performance requirements.

As students, legal savvy cyberworkers should:

1. Acquire the common body of knowledge for cybersecurity law and policy to include terminology, concepts, and specific legal terminology.
2. Acquire the common body of knowledge related to national and international laws related to cybersecurity and their differences.
3. Apply legal concepts in issues related to cybersecurity including cases/controversies unique to cybersecurity.

4. Identify and explain common legal issues related to cybersecurity.
5. Understand and explain procedural legal requirements relevant to cybersecurity.
6. Demonstrate the ability to use legal and policy knowledge by analyzing cybersecurity issues from a cyber worker perspective such as whether a security incident violates a privacy principle or legal requirement necessary for a valid response.
7. Demonstrate the ability to work through a case study identifying legal issues, analyzing the cybersecurity action required, and formulating a plan that complies with applicable laws.
8. Synthesize an action plan through analyzing cybersecurity legal and policy knowledge issues

Scope of the Issue and Analysis of the NIST NICE Framework: A search on the NIST NICE Framework using search terms of "legal;" "law;" "privacy;" "counsel;" "regulation;" "compliance'" "policy/policies" (an ambiguous term and used only in the context of government policies) "contract," "legislation," or "Executive Order," reveals a number of required tasks and KSAs throughout the seven Specialty Area Categories.

The initial analysis of the Framework found 72 tasks, 26 knowledge IDs, 6 skills, and 12 abilities that require some form of specific law and privacy knowledge. Although cursory , the analysis anecdotally identifies a surprisingly significant number of specialty areas requiring relevant KSAs for non-attorney work roles such as: (1) System Architecture (ARC): *"Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes." or* (2) Threat Analysis (TWA): "*Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities*."

Yet, only two work roles within the Specialty Area "Advice and Advocacy (LGA)" require a Juris Doctorate degree. The LGA specialty: "*Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain.*

Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings." The LGA specialty occurs in two work roles: (1) Cyber Legal Advisor (OV-LGA-001) who "*Provides legal advice and recommendations on relevant topics related to cyber law*; and, (2) Privacy Officer/Privacy Compliance Manager (OV-LGA-0021) who "*Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams*."

By comparison, many more work roles with their specialty areas require legal/policy knowledge such as: (1) "*Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy*." [K003]; (2) "*Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).*" [K0044]; or (3) "*Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations."* [K0107].

Workshop: We propose incorporating into the NACE Workshop a discussion on deriving the requirements for courses to address this substantial gap. The proposer taught the first-ever course at Texas A&M University in Spring 2018 addressing the need for legal savvy cybersecurity students. She proposes to offer that syllabus as a point of departure for the discussion. The workshop and its anticipated contribution to curricula development is essential to building analytical capabilities of future cyberworkers to operate within the dynamic and time constrained cybersecurity threat environment.

Additional Benefits: Developing these curricula may help to broaden the spectrum of applicable jobs and may increase the diversity of cybersecurity workforce. In addition to attracting those with engineering and IT skills, expanding the curriculum to develop legal and policy skills may attract students with different analytic and communication strengths, and as a result, both increase their number while improving the competency of the holistic workforce.

.

Paula S. deWitte, J.D., Ph.D., P.E.

Paula S. deWitte, J.D., Ph.D,. P.E., is both a Ph.D. in Computer Science and a licensed attorney in the State of Texas. She is a registered patent attorney with the United States Patent and Trademark Office (USPTO). She is one of less than 100 licensed Professional Engineers in the State of Texas in Software Engineering (SWE). She holds a Bachelors and Masters from Purdue University where in 2015 she was honored as the Distinguished Alumna in the Department of Mathematics, School of Science. She obtained her Ph.D. in Computer Science from Texas A&M University in 1989. She currently is the Assistant Director of the Texas A&M Cybersecurity Center and an Associate Professor of Practice in Computer Science and Engineering. Prior to joining Texas A&M University, she started several technology businesses. She most recently started two companies in oil and gas on a patented process in analyzing drilling fluids [US Patent US 8812236 B1] and has a patent pending through the European Patent Office (currently on review by USPTO) on incident response to a cybersecurity attack in the industrial control environment. She has mentored start-ups at Rice University OwlSpark and the University of Houston RedLabs. Before she joined Texas A&M University in July 2017, she was an Adjunct Professor at the University of Houston.

NACE Workshop
June 9-10, 2018
New Orleans, LA

The Role of Extracurricular Activities in Cybersecurity Education

In order to sustain the long-term needs of the cybersecurity workforce, more young people must be recruited to pursue cybersecurity-related careers. Career trajectories are often shaped early, even as early as middle school. It is therefore essential that more interventions and outreach efforts target these earlier age groups. Cybersecurity education is severely lacking at the primary and secondary school levels [1], and does not appear to be improving in any significant and widespread way. Most K-12 schools around the country are over-tasked and under-funded, and there is little room for new programs. While the "CS for All" initiative has gained some traction lately, it has been, and continues to be, a long uphill battle. It is unlikely that cybersecurity will ever be able to evoke the same broad appeal as an academic subject, and cybersecurity will almost certainly remain a rare subject in American primary and secondary schools for the foreseeable future. Therefore, the best way to introduce these young students to cybersecurity topics and careers has to be outside the classroom, with extracurricular educational activities.

Studies have found that extracurricular activities can have a significant impact on students' educational and career choices, and they can be an effective avenue for stimulating interest in specific career fields. Competition-style activities have been particularly successful at getting more students interested in STEM careers. A study of past participants in the National Ocean Sciences Bowl, for instance, found that 41% of respondents indicated that participation influenced their choice of career, and 39% said that it influenced their choice of college major [2]. Extracurricular competitions can also help launch talented students into highly successful careers. Winners of academic Olympiad competitions were found to significantly outperform their peers in various measures, and both participants and their parents agreed that the Olympiad developed their talent and fostered their future accomplishments [3]. These types of activities can help motivate students to pursue a subject and/or career, and to strive for excellence in that field. The activity can serve as an impetus to get the student started, and to help drive them toward

success when they get bored or frustrated. These activities also foster role-model relationships between professionals, who often serve as mentors and judges, and the students participating. Meaningful interaction with "real" practitioners can have a powerful impact on a young person. This is especially important for students who do not often receive exposure to a wide range of careers, and to students who may have difficulty seeing themselves in a particular career because their race or gender is underrepresented [4].

It is encouraging that competition-style extracurricular activities have been successful in other STEM fields, since competitions are already one of the most popular forms of cybersecurity activities. There are now dozens of cybersecurity competitions, both large and small, for varying skill levels [5]. One of the most popular is the Collegiate Cyber Defense Competition (CCDC), a national cybersecurity tournament for college students, with affiliated regional competitions [6]. CCDC has gained popularity especially for its value in creating hands-on learning experiences for students in cyber and computing related fields. It also has the potential to increase the inflow of new students into the cybersecurity profession, by recruiting, retaining, and identifying students who would be interested and adept in cybersecurity roles [5], [7].

As discussed earlier, however, college is too late for many students, who may have already chosen a different career path. It is important, therefore, to provide opportunities below the college level. The only truly national program of cybersecurity extracurricular activities for middle and high school students is CyberPatriot [5], [8], run by the Air Force Association, CyberPatriot bills itself as "The National Youth Cyber Education Program" [9]. The central element of the CyberPatriot program is the annual cyber defense competition, in its tenth season as of the 2017-2018 school year. Small teams of middle or high school students scour a virtual computer for vulnerabilities, such as viruses, backdoors, and incorrect security settings, then eliminate those vulnerabilities for points. These teams can come from public or private schools, homeschool groups, Junior ROTC programs, Civil Air Patrol units, or other approved youth organizations [8], [10], [11]. A recent study [12] demonstrated that participation in the CyberPatriot program leads to increased interest in cybersecurity as an educational or career prospect. Furthermore, that increased interest was found to persist over time, leading to significantly increased likelihood of actually entering the cybersecurity workforce. The CyberPatriot program is also contributing positively to correct the gender imbalance in the

cybersecurity workforce. Female students consistently make up over 20% of the competition–approximately double the industry average [13]–and despite lower initial interest in cybersecurity careers among female participants, this interest increased by an even greater amount than it did for males.

In addition to CyberPatriot's national program, there are many excellent extracurricular programs springing up around the country. Many colleges, universities, and other organizations host locally-organized cybersecurity camps for local students and/or teachers. These camps are often supported by GenCyber [14], a joint National Security Agency and National Science Foundation grant program that enables select camps to be offered free to participants. There are also numerous small, independent non-profit groups offering a variety of programs to local youth, based on the passions of their volunteers and the availability of donor funding. Examples of such programs include Cyber Warrior Princess (www.cyberwarriorprincess.org) in Ohio, GhostWire Academy (ghostwireacademy.org) in Texas, and many others. These programs and others like them give young people opportunities to delve deeper into cybersecurity, opportunities they would not have had through traditional education systems.

Another approach for using extracurricular activities to introduce young people to cybersecurity is to incorporate cybersecurity content into existing youth programs. Civil Air Patrol and multiple Junior ROTC programs have done this very successfully using the CyberPatriot competition. The Girl Scouts of the USA have recently announced their plan to introduce a series of age-appropriate cybersecurity badges to their programs. This is a great example of how other youth programs can add cybersecurity to their offerings as well; in fact, Scouting badges are frequently cited as the prime model for using badging to motivate learning [15], [16]. The Boy Scouts of America has a program for personal online safety education [17], though nothing currently for cybersecurity. A team of professionals and educators is working to change that by designing and proposing a new Cybersecurity merit badge [18]. The great advantage of incorporating content into well-established youth programs is the breadth of the audience. Participants in these youth programs often try different activities just because they are offered by the organization (and maybe to earn a badge), potentially setting them on a path toward a career they would not otherwise have considered.

Extracurricular activities are establishing themselves as the centerpiece of cybersecurity education for American middle and high school students, and this trend is likely to continue. It is

critically important that the cybersecurity community as a whole embrace and support these programs, and they should be considered a central aspect of the overall strategy for K-12 cybersecurity education.

References

[1] G. L. Peterson and B. J. Borghetti, "K-12 Cyber Security Educational Content Information Gathering," 2015.

[2] K. Bishop and H. Walters, "The National Ocean Sciences Bowl: Extending the Reach of a High School Academic Competition to College, Careers, and a Lifelong Commitment to Science," *Am. Second. Educ.*, vol. 35, no. 3, pp. 63–76, 2007.

[3] J. R. Campbell and H. J. Walberg, "Olympiad Studies: Competitions Provide Alternatives to Developing Talents That Serve National Interests," *Roeper Rev.*, vol. 33, no. 1, pp. 8–17, Dec. 2010.

[4] M. A. Ozturk and C. Debelak, "Affective Benefits From Academic Competitions for Middle School Gifted Students," *Gift. Child Today*, vol. 31, no. 2, pp. 48–53, 2008.

[5] Katzcy Consulting, "Cybersecurity Games: Building Tomorrow's Workforce," 2016.

[6] "National Collegiate Cyber Defense Competition," *National Collegiate Cyber Defense Competition*, 2017. [Online]. Available: http://www.nationalccdc.org/. [Accessed: 02-Mar-2018].

[7] P. Pusey, M. Gondree, and Z. Peterson, "The Outcomes of Cybersecurity Competitions and Implications for Underrepresented Populations," *IEEE Security & Privacy*, vol. 14, no. 6, pp. 90–95, 2016.

[8] G. B. White, D. Williams, and K. Harrison, "The CyberPatriot National High School Cyber Defense Competition," *IEEE Security & Privacy*, vol. 8, no. 5, pp. 59–61, 2010.

[9] Air Force Association, "Air Force Association's CyberPatriot: The National Youth Cyber Education Program," 2017. [Online]. Available: http://uscyberpatriot.org/. [Accessed: 20-Nov-2017].

[10] G. B. White, D. Williams, and K. Harrison, "Developing a National High School Cyber Defense Competition," in *CISSE '10 - Proceedings of the 14th Colloquium for Information Systems Security Education*, 2010, pp. 83–89.

[11] CyberPatriot Program Office, "CyberPatriot X: National Youth Cyber Defense

Competition Rules and Procedures." The Air Force Association, Arlington, VA, 2017.

[12] M. H. Dunn and L. D. Merkle, "Assessing the Impact of a National Cybersecurity Competition on Students' Career Interests," in *SIGCSE '18 - Proceedings of The 49th ACM Technical Symposium on Computing Science Education*, 2018, pp. 62–67.

[13] Frost & Sullivan, Center for Cyber Safety and Education, (ISC)2, and Executive Women's Forum on Information Security Risk Management & Privacy, "The 2017 Global Information Security Workforce Study : Women in Cybersecurity," 2017.

[14] "GenCyber," 2017. [Online]. Available: https://www.gen-cyber.com/. [Accessed: 31-Dec-2017].

[15] S. Deterding, "Gamification: Designing for Motivation," *Interactions*, vol. 19, no. 4, ACM, pp. 14–17, Jul-2012.

[16] B. Alberts, "An Education that Inspires," *Science (80-.).*, vol. 330, no. 6003, p. 427, 2010.

[17] Boy Scouts of America, "Cyber Chip." [Online]. Available: www.scouting.org/cyberchip. [Accessed: 15-Nov-2017].

[18] M. H. Dunn, R. J. Caruso, L. D. Merkle, and R. Trygstad, "Proposed Cybersecurity Merit Badge for the Boy Scouts of America (Poster)," in *SIGCSE '18 - Proceedings of The 49th ACM Technical Symposium on Computing Science Education*, 2018, p. 1085.

Author Bio

Michael H. Dunn is a cyberspace operations officer in the United States Air Force. He received a Bachelor of Science in Computer Science, with a specialization in Information Security, from the Illinois Institute of Technology (IIT), and a Master of Public Administration from IIT's Stuart School of Business. He was recently awarded a Master of Science in Cyberspace Operations from the Air Force Institute of Technology, where his research focused on the impacts of extracurricular cybersecurity youth activities.

Michael's Air Force career has included assignments at Creech Air Force Base (AFB) and Nellis AFB, Nevada, Wright-Patterson AFB, Ohio, and a deployment to Al Udeid Air Base, Qatar. He is currently assigned to the 333rd Training Squadron at Keesler AFB, Mississippi, as an instructor for Undergraduate Cyber Training.

In addition to his academic credentials, Captain Dunn also holds multiple information security certifications, including Certified Information Systems Security Professional (CISSP) and GIAC Certified Incident Handler (GCIH).

Co-Op Light:

Developing a Cyber Security Workforce through Academia-Industry Partnerships

The need for cyber security professionals in the workforce will only continue to increase and the existing shortfall widen (Fourie et al., 2014). There are not enough people to fill the open positions. Yet, there are individuals with an educational background in cyber security that are not being hired. They do not have the required experience in many cases (Caldwell, 2013). Thus, we see organizations struggling to fill positions in cyber security, but unwilling to hire those without experience. Coincidentally, these individuals will never obtain the experience in cyber security if some employers do not take a chance on them.

Some programs have been able to address this problem directly, such as the NSF's Scholarship for Service (M. E. Locasto, Ghosh, Jajodia, & Stavrou, 2011). It provides students with an opportunity to work for a governmental organization performing cyber security work in exchange for a commitment by the student to work for the organization for a certain number of years. The program has been very successful. However, it is not an attractive option for every student since the service commitment may seem too long for some or the pay too low.

Internships have also been available for some, but generally are more difficult to find as employers are reluctant to hire individuals with little or no experience, even for internships. Some students may end up performing cyber security related work in a computer science or information technology internship, which may later be leveraged for a more cyber security focused position within the same or a different organization. Although for those seeking a cyber security internship in the first place, this is not necessarily an efficient or effective pathway.

Therefore, new approaches are needed for cyber security, including the increased use of older approaches that have proven track records in other disciplines. One approach that has been effective has involved partnerships between universities and industry. An example of this being done at a high and intricate level is Northeastern's Co-op program that requires students

to alternate between semesters of academic coursework with semesters of co-op experiences. This typically begins the second semester of their sophomore year. Although highly successful and a model of effective co-op education, it does require a significant amount of coordination, relationship building with industry partners, and an institutional willingness to transform the educational structure of a university. Northeastern has been doing it this way for years and it works for them (Smollins, 1999). For other universities without this history, there may be significant bureaucratic and institutional hurdles to develop a co-op model for just one or more programs. Likewise, it can take several years to develop the necessary relationships, both within the institution and with external partners.

An effective approach for many universities may try and combine elements of internship programs with those of a co-op model to provide a more holistic educational approach to cyber security workforce development (Hoffman, Burley, & Toregas, 2012). One could think of this as "co-op light." This approach has been employed at some universities (M. Locasto & Sinclair, 2009), as well as the University of Washington under the coordination of the Center for Information Assurance and Cybersecurity (CIAC). During the initial stages of the development of this program, the University of Washington has partnered with a large corporation that has its headquarters in the region. This corporation has significant needs for diverse cyber security talent, including both technical and non-technical positions available.

To garner interest with potential participants, various information sessions are held on campus, such as the University of Washington Bothell campus. Given the diverse nature of cyber security positions available with this corporation, it is often a matter of finding the right fit between a unit or division of the corporation and high-caliber students. In other words, students apply to participate in the program. Various hiring managers within the corporation that represent these diverse units or divisions then look through the applicants to see if there is a specific fit for their needs. This approach helps maximize the experience for both the student and the corporation.

CIAC provides a point of contact for all participants that serves as a professional career advisor to them. If issues should arise, this individual helps troubleshoot them on behalf of the

student. Additionally, a cohort model is employed that allows for shared experiences between students as they enter the various components of the program together. This provides a peer-support mechanism for these students that can be invaluable.

Part of this cohort model includes the completion of additional academic coursework together. This three-course sequence results in a cyber security-related certificate from the University of Washington's Professional and Continuing Education (PCE) component. It also satisfies the requirements of CNSS 4011, CNSS 4012, and CNSS 4016. Thus, students walk away from this program with an additional credential and valuable work experience. For most, this has resulted in job offers for the student from the corporate partner with most of these offers being accepted. This is a win-win for the student and corporate partner.

Thus far, this program is in the process of completing its second cohort with the third cohort on the way. Part of the design of this program involves feedback from stakeholders and participants on a regular basis so that improvements remain ongoing and continual.

Several lessons have been learned and are continually being adapted and applied. For example, the three-course sequence that results in a certificate from PCE was a pre-existing certificate program that was not designed with the unique needs of program participants in mind. One possibility for the future may involve designing a certificate program that is custom designed for these students. The original decision to use a preexisting certificate curriculum was made to optimize the use of existing resources and to minimize program overhead, especially when the success of the model remained uncertain. As the program continues to demonstrate a successful overall approach, the development of a tailor-made certificate curriculum should be revisited.

Additionally, the program currently has one corporate partner. New corporate partners are being explored to build upon these initial successes. Diversification and expansion of corporate partners will be vital to ensuring the continued success of the program and provide a broader number of industries students with an interest in cyber security can pursue.

This program does not replace other successful programs, such as Scholarship for Service or full co-op models (e.g., Northeastern). Nonetheless, it does help fill a void. It provides greater flexibility as is often seen in internships, but with increased structure, learning opportunities, and a cohort approach, as is often seen in co-op models. The overall risk in participating in the program, whether as a student or as a corporate partner is also quite low compared to other models that have been employed in the cyber security domain. There will never be a one-size-fits-all approach to address the significant shortage in the cyber security workforce. However, by continuing to be creative and willing to take chances, additional voids can be filled and successes recorded.

References

Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud & Security*, *2013*(7), 5–10.

Fourie, L., Pang, S., Kingston, T., Hettema, H., Watters, P., & Sarrafzadeh, H. (2014). The global cyber security workforce: an ongoing human capital crisis. *Global Business and Technology Association*.

Hoffman, L., Burley, D., & Toregas, C. (2012). Holistically building the cybersecurity workforce. *IEEE Security & Privacy*, *10*(2), 33–39.

Locasto, M. E., Ghosh, A. K., Jajodia, S., & Stavrou, A. (2011). The ephemeral legion: producing an expert cyber-security work force from thin air. *Communications of the ACM*, *54*(1), 129–131.

Locasto, M., & Sinclair, S. (2009). An Experience Report on Undergraduate Cyber-Security Education and Outreach. In *Proceedings of the 2nd Annual Conference on Education in Information Security (ACEIS 2009), Ames, IA, USA*.

Smollins, J.-P. (1999). The making of the history: Ninety years of Northeastern co-op. *Northeastern University Magazine*, *24*(5), 19–25.

New Approaches to Cybersecurity Education (NACE) Workshop
Contact: Michelle Duquette duquettem@battelle.org 703-831-7413

Idea Submission

In order to address the shortage of a future cybersecurity workforce shortage, our efforts need to be focused on addressing the broader issue of technology education among our students. While children and young adults are presented with a multitude of electronic devices at home and in the classroom, the understanding of 'how' these devices work is lost. Without an understanding of 'how', how can we expect there to be understanding of the complex interactions and interdependencies within cybersecurity?

A video on YouTube, "*Teens React to 90s Internet"* with over 16 million views[1], depicts young adults experiencing an educational video about the Internet. They were asked questions about the meaning behind ".com" and ".org", and "How do you get on the Internet?" The young adults simply do not know how the Internet exists but simply that it is "just there." In addition to the problem of young adults not being taught, is the lack of technology teachers and curriculum to address the subjects.

I am proposing a mix of technical and non-technical topics discussed as part of every grade from elementary through high-school that advances in understanding and application as students progress. Younger grades are introduced to appropriate behavior, anti-bullying as part of activities that teach children right versus wrong; middle grades are focused on the parts and pieces that make up computers and the Internet, their functions and interdependencies; senior grades focus on theory, law, psychology and advanced certification studies.

Elementary / Grades 1-5

- Introduction to technology and appropriate behavior
- Game design through basic coding
- Cyberbullying

Middle school / Grades 6-8:

- Introduction to computer parts and pieces

[1]*Teens React To 90s Internet*, Published 01 June 2014 by REACT https://youtu.be/d0mg9DxvfZE

- Design theory through hardware deconstruction
- Technical drawing and network design

High-school / Grades 9-12:

- Combining the human element and technical function.
- Educating on landmark technical cases involving privacy (FBI Stingray), Computer Fraud and Abuse Act (CFAA)
- Historical figures (Alan Turing, Vint Cerf, Grace Hopper) and their contributions to computers and the Internet
- Workforce needs and education/certification requirements

In my work with high-school and college interns is the idea that "it's too hard" or, "it's not relevant to me" would consistently arise. Having been presented with topics such as the privacy control settings for popular smart phone apps, understanding what data types are generated from their interactions online and the value of that data, and even providing demos of hacks used via Wi-Fi, lead them to become more engaged on the subject and understanding that it does affect them and their everyday actions. Additionally, that the material was not difficult, only that they had yet to be presented with the information in a manner that was consistent with how they digest it (both visually through delivery and writing style).

While this level of interaction may not be possible to all students, I recommend a partnership with organizations that can provide the tools and resources to our education system. ISC^2 provides cyberbullying education directly with students, Palo Alto provides cybersecurity education to young girls through Girls Scouts while Disney, Khan Academy, and Tynker (among others) support 'Hour of Code' programs.

These programs are provided freely by both non-profit and commercial companies as part of a broader understanding of the need to teach our students these valuable skills. I propose requiring a larger commitment from commercial, non-profit and academia to provide education and training classes to high school students on cybersecurity. As students prepare to join the workforce, each individual is responsible for practicing 'good cyber hygiene' and it is within

these organization's best interests to ensure the next workforce understands their role and responsibilities to their employer regardless of their job title. It is also within these organization's best interest to interact with students on ethics, intellectual property, data breaches, risk management and consumer protections and privacy.

BIO

Michelle Duquette is a cybersecurity advisor supporting Government clients and Fortune 500 companies for over 10 years. Michelle has worked with integrated product teams and advised senior leaders on the issues of security engineering, Cybersecurity policy management, and information risk management across varying government classification levels. Michelle works as a Cyber Security Advisor with Battelle Memorial Institute and previously as a Senior Consultant for Booz Allen Hamilton, and a Software Engineer with Lockheed Martin.

Michelle holds both a M.S. in Computer Science and a Graduate Certificate in Information Assurance and Cybersecurity from George Washington University, and a B.S. in Information Management and Technology from Syracuse University. Michelle is a Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH). Michelle presented at the 2015 American Petroleum Institute 10th Annual Cybersecurity Conference on, "Biometrics: What is it and Where Do I Begin?"; published internationally in the July 2014 Information Systems Security Association Journal, "Our Children's Future: As Determined by Their Online Identity", and on the panel for TechWeekDC 2017 for 'Women Take on Careers in Tech' providing insight on how to start a career within cybersecurity in DC, perspective on how to create the career you want, and personal experiences.

Proposed College Curriculum Changes for Producing Secure Developers

Christine Fossaceca
MIT Lincoln Laboratory
christine.fossaceca@ll.mit.edu

The need for more robust software is evident from the increasing number of cyberattacks occurring daily. [1] However, the fear of sophisticated nation-state actors and zero-day vulnerabilities is partially misplaced. Although these are formidable enemies, companies and governments should be more concerned about a major threat from the inside: poorly constructed code. A search of the 2017 CVE database shows that there are still new buffer overflow vulnerabilities being found [7], despite those being among the most basic type of exploits. This leads to the question: Why are developers still implementing programs with simple vulnerabilities?

The first place to look may be the educational background of software developers. One major problem is that students who want to become software engineers see cybersecurity related courses and think, "That doesn't apply to me". Then those students become developers, leaving security concepts to be implemented by a "security team". Security researcher Sarah Zatko gave a presentation [5] at the Hackers of Planet Earth (HOPE) Conference in 2014 diagnosing this systemic issue as "security afterthought syndrome", and lamented that cybersecurity isn't prioritized by many professors or taught by universities. Two years later, Professor Ming Chow of Tufts University and his colleague, Professor Roy Wattanasin of Brandeis University, replied to Zatko at HOPE 2016 [3], where they discussed being inspired by her presentation and made changes on their own campuses to address cybersecurity in computer science education.

In order to determine if other colleges and universities were following the urgings of experts in the security community by making curriculum changes, I recently conducted a survey of over 100 colleges and universities in the United States and presented the results at the IEEE Secure Development (SecDev) Conference. I worked with two of my interns at MIT Lincoln

Laboratory, and we reviewed the Computer Science curriculums of select schools, which were chosen based on their US News and World Report Rankings [6]. The schools were in the 2017 listings for "Top 50 Nationally Ranked", "Top 50 Regionally Ranked", and "Top 50 Computer Science Programs".

In the first part of the research, we looked at every curriculum and course description, searching to see if any required courses had the word "security" in the description. We found that 97 percent of computer science programs had at least one course that mentioned the word security in the description, however, only 31% of schools actually required one of those courses in their curriculum. Furthermore, it was determined that the word "security" is too ambiguous to rely on as a metric, as word "security" meant cryptography, network protocol security, privacy, forensics, or cyber policy, just to name a few categories discovered in the survey.

In the second part of the survey, we looked at the accreditations of the schools, and noted that the majority of top tier schools were ABET accredited (50% of Regionally Ranked schools, 92% of Nationally Ranked schools, and 94% of the Top Computer Science schools). This suggests that the ABET committee drives the curriculum requirements for these schools. A search of the ABET computer science curriculum turns up a requirement for computer science programs, "To have an understanding of professional, ethical, legal, security, and social issues and responsibilities." [4] Although some schools didn't have ABET accreditation, they usually had another accreditation listed on their website, and their curricula were quite similar to those of the ABET schools.

We are producing more software than ever before, in a landscape where there are also more malicious actors, so most software developers unknowingly have a target on their backs. We have to start preparing college students to enter the increasingly adversarial environment of the Internet by building security concepts into computer science and engineering education. Although there will always be new kinds of cyberattacks, computer science students should be well-informed about old attacks. As an example, students who are learning C programming should not be taught to use strcpy() without learning what a buffer overflow is. This issue was addressed in 2010 by three Carnegie Mellon professors who were planning to implement

changes in the Computer Science curriculum to increase "our emphasis on the need to make software systems highly reliable." [2] Today, freshmen at Carnegie Mellon do, indeed, learn buffer overflow vulnerabilities in the required course 15-222 Principles of Imperative Computation, where students focus on the "correctness of programs", not "security".

I assert that graduating computer science students who go on to become software developers without learning secure coding practices ahead of time are left to learn on the job, and when a more experienced developer isn't auditing their work, another simple bug is implemented in production code, waiting to be discovered by the adversary. It is proposed that more schools follow the model of Carnegie Mellon in teaching secure programming techniques. To do this, reaching out to accreditation establishments and advocating for changes in curriculum requirements is necessary, as well as promoting the use of phrases such as "correctness of code" and "expected execution" rather than the vague word "security". This will in turn produce graduates who will be less likely to write programs with commonly known vulnerabilities.

References

[1] 2017 Internet Security Threat Report. Symantec Corporation, Apr. 2017, www.symantec.com/security-center/threat-report.

[2] Bryant, Randall E., Sutner, Klaus and Stehlik, Mark J. "Introductory Computer Science Education at CarnegieMellon University: A Deans' Perspective." Aug. 2010, www.cs.cmu.edu/~bryant/pubdir/cmu-cs-10-140.pdf.

[3] "Computer Science's Curricula Failure-What do we do now?" Chow, Ming and Wattanasin, Roy. HOPE 2016

[4] "Criteria for Accrediting Computing Programs, 2017-2018." *ABET*, Accreditation Board for Engineering and Technology, 2017, www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2017-2018/.

[5] "How to Prevent Security Afterthought Syndrome". Zatko, Sarah. HOPE 2014

[6] *Rankings and Advice*. U.S. News & World Report, 2017, www.usnews.com/rankings.

[7] Security Vulnerabilities Published In 2017." CVE Details Search, MITRE Corporation, 2017, www.cvedetails.com/vulnerability-list.php?vendor_id=0&product_id=0&version_id=0&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=2017&month=0&cweid=0&order=3&trc=9201&sha=815cc1a3d2c4b72bf23b8a2fa85939f5ab0041c0

Bio

Christine Fossaceca is a cybersecurity researcher at the MIT Lincoln Laboratory, focusing on tool creation, exploit development, vulnerability research, and reverse engineering. She first became interested in cybersecurity education when she entered the workforce as a recent graduate and started feeling overwhelmingly unprepared to write "unhackable" code. In speaking with other recent graduate friends, she noticed a trend among software developers to rely heavily on "security teams" to pentest their code for them in the deployment process, rather than the developers themselves following any particular set of secure coding practices. In her discussions, the nervous laughter of her colleagues usually covered up a real fear of causing a major security breach because the review team didn't patch something. She started to question, "Why did my professors even teach me strcpy()? Why didn't the databases course include a section where we tried to perform SQL injections on our classmates? Why didn't any of my classes encourage me to use a debugger like gdb?" After becoming interested in the topic, she became involved with the IEEE Secure Development conference (IEEE SecDev) and formed a group on improving security education with collaborators from Google and Tufts University.

Improve Cybersecurity Education by Bringing Secure Coding to CS1

New Approaches to Cybersecurity Education (NACE) Workshop, June 9 & 10, New Orleans, LA

Simson L. Garfinkel

The United States is utterly dependent on information technology, but only a fraction of the those working in computing specialize in cybersecurity. The reason is that the field of computing is tremendously broad. Just as there are now dozens of cybersecurity specializations, there are now dozens of computing specializations as well.

Consider the numbers from the 2016 Taulbee Survey, the annual survey by the Computing Research Association that tracks PhDs in computer science, computer engineering and information.[1] Of the 1888 students graduating in North America with a relevant PhD in 2016, just 106 (5.6%) found employment in "security/information assurance" — yet "security/information assurance" was the second largest employment category reported on the survey (only exceeded by Artificial intelligence). There are simply too many aspects of computing systems that require teaching and researching: security is critical, but so are the other specializations.

If our goal is to improve the state of cybersecurity using the lever of education, then we must consider ways of broadening cybersecurity education to include non-specialists. That is, we need a longer lever. This means incorporating security education throughout the entire computing curriculum, starting with the first computer science course that students take, affectionately called CS1 in the literature.

It has long been observed that many CS1 courses have programming examples that contain serious, exploitable security errors. In the days of "C" it was common for instructors to present programs with buffer overflow errors. These days, it is common to present programs that allow for brute-force password guessing, or SQL injection attacks, or just horrible usability that promotes unsecure use. We also have poor security practices in many educational computing environments—such as easy-to-guess passwords, open services, web services protected by hidden URL, and so on—in the interest of expediency.

[1] https://cra.org/crn/wp-content/uploads/sites/7/2017/05/2016-Taulbee-Survey.pdf

Programming examples with vulnerabilities and poor security practices in these introductory courses is poor pedagogy. We shouldn't be teaching the students with practices that we wouldn't want them to repeat on the job. We must scrub introductory courses of poor examples, and instead assure that these courses demonstrate good security practice. This will almost certainly require that security faculty partner with other faculty who teach the introductory courses.[2] [3]

As the need for programmers continues to expand, programmers who do not have the benefit of formal security instruction will be creating most of the code that powers our society. These programmers will use the tools of their trade. If introductory courses incorporate sophisticated security technology, it will be reflected in popular tools, there will be a multiplier effect. The result will be more code with fewer exploitable defects.

Other modern software engineering practices have been incorporated into introductory courses with great success, including test-driven development, continuous integration, and distributed source code control. These practices have been adopted because they make programmers more efficient and decrease software defects—and in the process, help to make software more secure.

Likewise, introductory programming courses should teach code annotations to support model checking, the use of static code checkers, and lightweight formal methods.[4] These techniques will be sold to students (and their teachers) as ways to make software more reliable and software development more efficient. As a side effect, their code will also be more secure.

April 26, 2018

[2] K. Nance. "Teach them when they aren't looking: Introducing security in CS1." IEEE Security and Privacy, 7(5):53–55, Sept. 2009.

[3] V. Pournaghshband, "Teaching the Security Mindset to CS 1 Students," SIGCSE'13, March 6-9, 2012, Denver, CO.

[4] K. Schaffer, J. Voas, "Whatever Happened to Formal Methods for Security," IEEE *Computer,* August 2016.

Integrating Cybersecurity into the K-12 Classroom

We are living in the midst of a social crisis as technology rapidly expands and bad actors take advantage of our democratic system. America's belief in the power of liberty and open systems comes with drawbacks such as opposition to preemptive, offensive, or aggressive actions taken in the field of cybersecurity by our own government officials. Achieving the balance between liberty(privacy) and security is a challenge. As a country we should strive to "future" proof the education provided in cybersecurity. To achieve this worthy goal an emphasis on teacher development and an intentional expansion of resources into the K-12 environment must occur. A job shortage of a predicted 1.8 million people by 2022 (CSO Online, 2015) and the increased need to teach digital natives basic cybersecurity survival skills, (Irish Times, 2018) require that cybersecurity be integrated in a multidisciplinary fashion in the K-12 classroom. Educating the populace in the field of cybersecurity is necessary for three concrete reasons: 1. To prepare students for an ever-increasing technology-based future; 2. To expose students to the jobs and careers available in cybersecurity; 3. To defend our nation from the many types of cyberwarfare tactics performed by America's adversaries. This initiative can best be started in the K-12 system.

Multiple stakeholders must be involved in order to develop the most impactful, institutionalized design possible; a design that impacts the most students while still allowing the individual classroom teacher freedom to be creative and adaptive. If this crisis is left solely to politicians, it may fail.

The following model is presented for discussion, debate, and open dialogue:

a. Establish regional teacher learning communities, sometimes referred to as professional learning communities. This is a recognized best practice that can both enhance teacher quality as well as empower teachers to lead. Teacher quality is the single most important factor when determining student success in the classroom. A teacher learning community (TLC) is not a staff meeting. Instead, a TLC focuses on collaboration, continuous improvement, and a growth mindset in

CSO Online: http://www.csoonline.com/article/2953258/it-careers/cybersecurity-jobmarket-figures-2015-to-2019-indicate-severe-workforce-shortage.html
Irish Times Online: https://www.irishtimes.com/news/education/the-myth-of-digital-natives-1.3459381

order to both teach the educator new skills as well as allow a place for dialogue. Within a TLC, teachers can share strategies and lessons that work as well as share items that do not work. This teacher-centered approach improves educator awareness and quality in order to benefit student learning. These TLCs also could create ideas for incorporating a standard based, multidisciplinary cybersecurity curriculum throughout the United States.

b. In order to be impactful, these TLCs will need a relationship with post-secondary academia and local cybersecurity experts. It is suggested that each TLC be led by at least one master teacher in each region. This master teacher would serve as a link between higher education, government/industry, and the K-12 environment as well as be responsible for leading established monthly professional development sessions on cybersecurity topics. The master teacher would need basic cybersecurity knowledge and serve to help others learn and adapt for individual disciplines.
c. All teachers will also need access to a shared online database or website to share and explore lesson plans. This website would allow interested teachers a "one stop shop" to explore lesson plans and activities for the K-12 classroom. Teachers would also be encouraged to adapt posted lessons and/or share new lesson plans to create the best resource possible. Contained within this website will be a cyber-ethics module for students in each grade band (grades 3-5; 6-8; 9-12). This ethics module could be used by all disciplines and all teachers in the K-12 classroom to instill necessary ethical guidelines.
d. After the establishment of the TLCs, a grant program could be established to bring longevity and a local approach to teaching cybersecurity within each school district. Under this proposal, interested school districts could apply for grant money to fund one cyber literacy outreach coordinator for the district. Responsibilities of this individual would mirror the established practice of utilizing instructional coaches within the K-12 setting. The cyber literacy outreach coordinator would "coach" individual classroom teachers in lesson development, hands-on activities, and co-teaching opportunities to both create new lessons and implement cybersecurity topics into current lessons. This person would also be responsible for attending professional development opportunities such as the

NICE K-12 conference to stay current and up to date on cybersecurity trends. The instructional coaching model has proven to be effective. Instructional coaches help teachers become better teachers by facilitating creativity and best practices. Better teaching methodology leads to higher student production.

e. Continuous in-person professional development should occur in the form of one-day cybersecurity boot camps that use the "teach the teacher" model. These events could occur in each region to begin the process of institutionalizing cybersecurity concepts into the classroom. The one-day boot camps would advertise to all teachers regardless of discipline or experience. A beginner session; along with an advanced session would be offered. Not only is there a desire amongst teachers who lack experience, but experienced technology/CS teachers strongly desire guidance in implementing cybersecurity into their coursework. Some teachers may not have the time or desire to commit to a TLC. However, completing a one-day session may encourage them to join the community.

The strategies described in this document are already being used; only the content topic has changed. Placing an increased emphasis on funding cybersecurity education initiatives in K-12, utilizing proven teacher development strategies, and establishing a community of multidisciplinary cybersecurity advocates within the K-12 setting will institutionalize the process of educating students on cybersecurity at a young age. These actions will solve the job shortage crisis, make Americans better cyber citizens, and prepare the nation for the ongoing struggles with foreign adversaries and bad actors.

Biography

Ms. Ashley Greeley received both her Bachelor's and Master's degrees from Purdue University. She began her teaching career in 2003. After two years in the special needs classroom, Ms. Greeley began teaching social studies at Harrison High School (West Lafayette, IN). While at Harrison, she developed two new courses for insertion into the curriculum (AP US history and AP US government), coached a variety of sports and an academic team, served as both department and corporation chair, led the school improvement team, facilitated teacher professional development, and served in whatever capacity asked of her. Greeley was awarded numerous teaching awards and recognition including the Golden Apple, the DAR History Teacher of the Year, the Indiana Historical Society Teacher of the Year, the Indiana History Teacher of the Year, the Indiana representative at the Supreme Court Summer Institute, and was a top-25 finalist for the Indiana Teacher of the Year Award. Beginning in 2015, Greeley began serving as a site visitor for GenCyber summer camps. In 2017, Ms. Greeley was awarded an NSA/CAE grant to develop a multidisciplinary K-12 cybersecurity curriculum as well as perform cybersecurity outreach for Tippecanoe School Corporation as an extension of the INSuRE program at Purdue University.

Meeting the Cyber Security Workforce Demand

By Drew Hamilton

Mississippi State University

Twenty years ago it was reasonable to think that the demand for computer security would crest as technological innovations secured what we now call cyberspace and our connection points into cyberspace. It was tempting to remember studies cited in the first information systems courses in the sixties showing curves that indicated that eventually every man, woman and child in the United States would need to become switchboard operators in order to meet projected demands. Of course that did not take place – technology replaced the vast majority of human telephone operators.

Currently, new technology is actually *increasing* cybersecurity workforce demands and broadening and deepening the skill sets required for the cybersecurity workforce – quite the reverse from the telephone operator issue. In this short paper, we will consider the following issues:

1. CyberCorps and its impact on the US Civil Service, the private sector and a revived DOD Information Assurance Scholarship Program (IASP)
2. Education versus training
3. New Technology and Cybersecurity education
4. Future Directions

1. CyberCorps and its Impact

The impact that the NSF CyberCorps program has had on the Federal cybersecurity workforce has been well-documented elsewhere. There has also been a positive impact on state, local and tribal governments. In many rural areas, the only way a state or local government entity can make a quality cybersecurity hire is with a Cybercorps graduate who has a service obligation and wants to stay close to home.

Early in the days of the SFS program, some PIs were encouraged to prioritize placements in non-DoD Federal Service. At that time, the DoD IASP was running a similar program, but one where student scholars were selected by the DoD agencies where they were expected to intern and then serve out their service obligations. But the DOD IASP did not consistently produce close to the number of scholarship students as SFS. With rumors of a revival of the DoD IASP, it may make sense for the DoD program to specialize in DoD-unique and mostly DoD-unique cybersecurity skills such as attack, exploitation and intelligence tradecraft.

While SFS has clearly impacted the Federal workforce, it has also had a major impact on the US private sector workforce. SFS enabled its Federal sponsors to "lock up" the best student talent early and commit them to government service. Industry has paid attention. Tech firms, particularly Tech giants Facebook, Amazon and Google are actively engaging with undergraduate students looking for talent with internships, co-ops and contract work during the semester. This is formidable competition because the tech giants have deeper pockets and fewer constraints then Federal agencies.

2. Education versus training

The critical shortage of cyber security workers has contributed to the rise of cyber security certification business. DODD 8140 (and its predecessor DODD 8570) ensures a government requirement that must be met. Additionally, non-defense industry also seems to favor graduates who have earned commercial cyber certifications such as Security+, CEH, CCNA-sec, etc.

Training, "the action of teaching a person or animal a particular skill or type of behavior" differs from education, "the process of receiving or giving systematic instruction." You can train someone to program in Ada and you can educate him/her in computer science to include programming skills. We train programmers in specific languages/environments and educate software engineers. Training is important, but tends to be of shorter-term value. Training strategies can

certainly be used as a stopgap measure to address critical personnel shortages. The Cybercorps program must remain focused on educating the cybersecurity workforce. Federal agencies may need to train new hires in specific skills Education is needed to provide the foundation for life long learning. Education on fundamental principals is the only way to "future proof" the education we can provide. Consider Coffman and Denning's 1973 classic *Operating Systems Theory*. It won't train a student on the Windows registry but the operating system design principles espoused in this work are still valid fifty years later.

3. New Technology and Cybersecurity education

University cyber security programs are challenged with having an increasing number of topics to cover. The NSA CAE Cyber Operations Program is an example of a specialized set of cyber security knowledge units that incorporate both current subjects as well as older fundamental subjects such as assembly language programming and reverse engineering as well as cyber operations tradecraft. The result is an academic program that is difficult to fit into a traditional degree program.

The NSA CAE-CO program is clearly geared to the production of cyber security scientists and engineers. While NSA is focused on the deeply technical side of cybersecurity, NSF CyberCorps meets a broader range of Federal government requirements including cyber security policy and information systems focused cyber security programs. An early lesson learned from the NSA CAE – CO effort is that it is very difficult to get deep coverage of all desirable cyber security skills in a single degree program. In NSA's case, there is also a need for its cyber security workforce to have specialized knowledge of intelligence tradecraft.

But the needs of the NSA are not necessarily representative of the entire Federal workforce. Different agencies have different cybersecurity workforce demands that are not all engineering based. Here is where the private sector needs differ from the public sector. Industry is demanding cybersecurity scientists and engineers and has much less demand for cyber policy and other "softer" cyber security skill sets.

New technologies are complicating this challenge. We are long way from having a single computer security course in a computer science program that was the norm fifteen years ago. Cyber security in software applications has expanded into other engineering disciplines and other colleges. Cyber security for SCADA systems, industrial control systems, IoT devices and High Performance Computing assets all require deep, specific technical knowledge that likely will lead to more and more specialized cyber security education and training programs. CyberCorps will receive applications from some of these newly formed, specialized programs and will need to consider whether these programs should become part of the SFS Scholarship program. This will further complicate the tradeoffs between technically and non-technically based CyberCorps educational programs. Should CyberCorps be cognizant that industry demands for cyber security professionals differs from government demands and plan accordingly?

4. Future Directions

ABET's recent move to accredit cybersecurity engineering academic programs is an important development. Future Cybercorps solicitations may wish to consider ABET accreditation in cybersecurity when evaluating new programs, particularly programs that do not fully meet the CAE criteria.

The author of "Dilbert," Scott Adams when asked, when asked if he had any advice for engineers, replied, "Engineers should work in organizations that value engineering." Having personally retired from Federal Service I doubted that government service would value engineers. However cyber technologies are rapidly changing that. NSA is clearly an organization that values engineers. Cyber technology is changing the Federal workspace and the security challenges are not only coming from amateurs and fraudsters, but also from nation state actors. While technology alone may not be sufficient to change attitudes in the Federal workspace, CyberCorps can and has. As more and more CyberCorps graduates rapidly advance

to leadership positions in the US Civil Service, they bring a new perspective to Federal cyber security that must continue to be nurtured.

Hamilton Bio-Sketch

Drew Hamilton is the Director of the Center for Cyber Innovation at Mississippi State University, a professor of computer science and engineering and leads the MSU NSF CyberCorps program. Previously he served as an Alumni Association Professor of Computer Science and Software Engineering at Auburn University where he initiated and led Auburn's SFS Program. He previously held faculty appointments at the US Military Academy and a visiting appointment at the US Naval Postgraduate School. Dr. Hamilton earned his doctorate in computer science from Texas A&M University. Dr. Hamilton is a distinguished graduate of the Naval War College

New Approaches to Cybersecurity Education Workshop

June 9-10, 2018, in New Orleans, LA

Proposal Submitted for the Steering Committee's Consideration

From Seth Hamman, Ph.D.

Author Academic Bio

Seth Hamman received the B.A. degree in religion from Duke University in 2002, the M.S. degree in computer science from Yale University in 2011, and the Ph.D. degree in computer science from the Air Force Institute of Technology in 2016. He is an Assistant Professor of computer science with the School of Engineering and Computer Science at Cedarville University. His research interests include improving cybersecurity education, and he has written journal articles and presented at national cybersecurity education conferences on the importance and practice of teaching adversarial thinking for cybersecurity. He has also been the recipient of two NSA National Cybersecurity Curriculum Program grants to develop curriculum for teaching adversarial thinking for cybersecurity and for teaching the legal and ethical aspects of cybersecurity.

Cybersecurity for All CS

The discipline of computer science is no longer in its infancy, but at only around 50 years of age, it is still in some ways in its adolescence. One of the next steps in its maturation must be for it to fully embrace security as a core part of its identity.

Because the benefits of "technology" (hereafter a catch-all term for the products of computer scientists) increase when they are networked together, the coming era of the Internet of Things is an inevitability. As this era comes about over the next decade, the distinction between technology and cyberspace will practically disappear. Therefore, securing cyberspace (i.e., cybersecurity) will be a concern of the vast majority of the next generation of computer scientists.

The movement of all technology into cyberspace is somewhat disconcerting because many of the properties intrinsic to cyberspace make it a fundamentally vulnerable domain. For example, cyberspace is *distanceless*, meaning that bad actors can operate at anytime from anywhere in the world, making the number of potential threat actors virtually limitless. Also, the world of cyberspace is *digital*, making it possible to perfectly impersonate others and trivial to steal, modify, and destroy cyberspace assets. Cyberspace is also *invisible*, cloaking nefarious activities in darkness. This makes it difficult to detect and to identify bad actors, enabling them to act with near impunity. These attributes (among others) combine to make cyberspace particularly susceptible to criminal wrongdoing, and history has shown that criminal bad actors are ready and willing to take advantage of these dynamics. These attributes also make cybersecurity, which is about protecting the rights of individuals and organizations in cyberspace, an enormously difficult undertaking.

Therefore, as cyberspace more and more becomes part of the core infrastructure of our society, all those involved in producing and deploying technology must be thoroughly security-conscious. Cybersecurity should be seen as a shared responsibility among all those involved in creating its artifacts and infrastructure. However, it is not clear that today's computer science programs are sufficiently emphasizing security to the extent that every graduate is security-minded. From my experience as a computer science faculty member and as a computer science graduate student over the past 10 years, security within the discipline of computer science is

still seen as something of a sub-discipline that some will focus on, while others are free to ignore. Again, this is especially disconcerting because increasingly, the proper functioning of our economy, the well-being of our citizenry, and the safe-guarding of our freedoms are all dependent on a secure cyberspace.

It is true that much progress has been made to raise awareness of this need within the discipline of computer science. For example, the CS Curricula 2013 guidelines made headlines for highlighting security as both a stand-alone and a cross-cutting concern. This was the first time in the history of the guidelines where security was specifically called out and represents a major step forward. However, the guidelines did not go far enough in emphasizing the importance of security. For example, the only time the word "security" is mentioned in the *Characteristics of Graduates* section, is under the *Familiarity with common themes and principles* sub-heading. The sub-section states, "Graduates need understanding of a number of recurring themes, such as abstraction, complexity, and evolutionary change, and a set of general principles, such as sharing a common resource, security, and concurrency." Again, it is good that security is mentioned in the context of characteristics of graduates, but the level of prominence assigned to it does not match its importance. In order to help create a more secure technological infrastructure, "security-minded" must be one of the foremost "characteristics of graduates."

Today we lament the fact that security concerns have frequently been an afterthought in the design, production, and deployment of technology, which has helped to lead us into an entrenched dependence on a vulnerable infrastructure. But with the current state of computer science education, these mistakes are likely to be reproduced by the creators of tomorrow's technology.

I recognize that this idea is not new. In fact, Eugene Spafford wrote about how computer security issues pervade every aspect of computing in the 90's in his testimony that in part inspired this upcoming NACE workshop. But I am arguing that to date, we (the cybersecurity education community) have not sufficiently prevailed upon our computer science colleagues to accept responsibility for incorporating security into their courses. This negligence has helped lead us into the present situation in the workforce where cybersecurity specialists

are continuously putting their fingers in a dike with new leaks sprouting around them all of the time. A continued push to raise awareness and ultimately to reorient the discipline of computer science around security is for me one of the most effective ways to deal the acute cybersecurity labor shortage.

Practical Next Steps

In order for computer science education to properly prepare the next generation of computing professionals, who are increasingly laying the groundwork for a technology-based society, the next stage in the maturation of computer science must focus on nurturing a security mindset in students. Producing a computer science graduate who is unconcerned with potential adversarial actions is like producing an accountant who does not appreciate the potential for an audit, or like producing a mechanical engineer who is not preoccupied with safety concerns. In short, it is irresponsible. Cyberspace is rife with threats, and no computer scientist should be enabled to remain ignorant of this fact.

I am not suggesting that cybersecurity should not be a specialized sub-discipline of computer science – it definitely needs to be, and I am sure that the NACE workshop will find ways to promote this from K-12 through graduate school education. I am also not arguing that every computer science graduate must be a cybersecurity specialist. But what I am suggesting is that every computer science graduate must be exposed to security concerns early in their course of study and throughout their program. It must be impressed upon every student that in addition to their expected user base, nefarious people exist with impure motives, and the threat they pose must be mitigated at every opportunity. We have done well at emphasizing reliability testing and the necessity for handling random natural events and unintentional human mistakes (which ported naturally from the discipline of engineering), but computer scientists must always consider potential adversarial actions as well (which is not a vital concern of most engineers).

We must work to promote cybersecurity among broad audiences of computer science educators. Already existing curricular guidelines like CS Curricula 2013 and CSEC2017 provide the specifics; our task must be making sure guidelines like these rise in prominence. One practical idea would be to push for security-related keynote addresses at future SIGCSE

conferences. Another idea is to work with ABET's Computing Accreditation Commission to better highlight and enforce security-mindedness as a student outcome. Teachers and faculty members reproduce what they are, and many of them are not security-minded, so another idea would be a to offer continuing education in the areas of cybersecurity for computer science teachers and faculty. Offering a free cyber workshop at major computer science conferences might be a great investment for equipping computer science faculty.

Preparing CyberSecurity Experts as Adjunct Faculty to Teach at the Post Secondary Level

Shelly Heller, Lance Hoffman and Costis Toregas
The George Washington University
Washington DC 20052

It is a well published concern that in order for the United States to maintain and expand its capabilities in the world of cybersecurity – whether planning new technologies and the internet of things (IoT), preparing defenses, constructing offensive tactics, or appropriate policies – a well-educated workforce is needed. To fill the numerous government jobs, many educational pathways have to be opened – including job training, community college programs and traditional four year and graduate programs. Each of these avenues educates and trains individuals to work at different levels and in different capacities in our 'cyber' world. Currently there is a capacity issue: students cannot readily be added to the education system, especially at the community college level, because trained faculty are scarce. The weak link in the cybersecurity workforce supply chain is often finding faculty who can be effective and provide the proper encouragement to students to join the cyber workforce. Therefore, success depends, in large part, on the capacity of our educational institutions to scale up and absorb increased numbers of students, as well as the capabilities of our educators.

The nation is looking to our community colleges as an untapped source of cybersecurity workers. According to the National Science Foundation, "Community colleges can play a critical role in giving students the hands-on skills that are needed on the front lines (of) defending computer networks[i]" According to the American Association of Community Colleges, there has been huge growth in the percentage of higher education faculty teaching in community colleges and the biggest group contributing to that growth are part time faculty. And, while some community colleges have existing programs in cybersecurity and have dedicated full time faculty, according to the Center for Community College Student Engagement, more than 58% of community college classes are taught by adjunct faculty. While the data is not broken out by discipline, an informal conversation with local community colleges is that they rely heavily on adjunct faculty, and many adjuncts may have no teaching experience. A typical advertisement for a cyber-security faculty member at a community college includes "Bachelor's degree (Master's preferred) and five years of work experience as Computer Forensics professional, technical qualifications: (CompTIA Network+, CompTIA Security+, CISCO certifications, CISSP, SANS, Certified Ethical Hacker (CEH)), knowledge of Programming Languages, excellent written and oral communications skills, experience in leadership including a history initiating and managing change, working with others toward shared goals and developing others." These

requirements can act as a barrier to many aspiring faculty members, thereby extending the mismatch between demand and supply.

Our answer: Tapping into cybersecurity experts as adjunct faculty. Cybersecurity experts in the workforce have the potential to fill the need for part-time cybersecurity faculty at the community college level. By tapping into the pool of working cyber security experts and retired individuals from government positions whose background fits the typical qualifications listed above, a viable long term strategy can be developed. These men and women, as government or private sector employees, often have had access to the latest technologies, wrestled with the current problems and policies facing the nation, have taken leadership roles and have a wide network upon which to rely for developing academic and career goals. In fact, they work with cybersecurity content on a daily basis.

Currently the Cybersecurity Teaching Corps project is exploring these possibilities through a research effort and a pilot "Teaching Cybersecurity at Community Colleges" online course (See Figure 1) funded by the U. S. Defense Department[ii]. While CyberCorps graduates generally possess the requisite cybersecurity content knowledge and experience to teach at a Community College level, they typically do not have teaching experience or knowledge of diverse learning and assessment techniques. Furthermore, most CyberCorps alumni are not a product of the community college pathway and they do not know the community college student and their unique challenges/opportunities. One can target the Cybersecurity Teaching Corps course to CyberCorps alumni with 3 to 5 years of work experience to address the typical requirements for adjunct faculty in community colleges or more broadly, to expand available adjunct faculty at four-year colleges and elsewhere.

introduction to Community Colleges, Ethics and general structure of a course
The typical Community College student, Faculty codes, Crafting goals and objectives
Teaching concepts – moving from concrete to abstract
Teaching concepts – using group work in your class
Teaching concepts – using case studies in your class
Teaching concepts – using discussions during a class

Figure 1: Cybersecurity Teaching Corps Course Content

[i] NSF (2013) Available on the web on December 8, 2016 https://www.nsf.gov/news/special_reports/science_nation/cybersecurity.jsp

DOD Grant: Grant# H98230-17-1-0371

NOVA | Northern Virginia Community College

April 30, 2018

Dear Sir/ Madam,

Here is a short submission for answering questions posted for this year's NACE Workshop. Due to seeing call of ideas late, I have only some ideas for consideration that I can expand should the committee want to hear more.

After teaching at George Mason University (GMU) and Northern Virginia Community College (NVCC) cyber and information assurance programs, students appear to lack the models and direction needed to develop into cyber professionals that have the foundations needed for success. Having a Model Activity Path (MAP) where students would see how the skills, classes, experiences link to actual work and needs in cybersecurity would make sense versus the traditional academic plans. Cybersecurity is truly a multifaceted domain that can be separated into areas such as policy, forensics, research, hardware, and other areas along with technical skills. Having MAPs developed by industry that features the skills and experiences employers foresee now and for the future would make the time, cost, and effort more relevant to students.

While many educational institutions have career paths and program curriculums, mapping those to actual work and careers is a challenge. As a hiring manager for a science and technology company, I have hired former GMU and NVCC graduates who perhaps use 20% of their education toward meeting client needs. As college is an exploratory along with development time for students, having MAPs developed along the lines of professional tracks would give students a visualization of where they can be upon matriculation. The MAPs would be developed through engaging industry to understand what is needed to "future-proof" the skills while helping educational institutions plan resources and classes. MAPs would also help level set the perceptions of cybersecurity toward reality versus fictional Hollywood versions of cybersecurity. For example, not all cybersecurity professionals are hacking or doing technical work.

An example of the MAP could be a Cyber Security Policy Analyst (CSPA). The MAP would encompass building skills in writing, legal research, sociology, and some technical courses. CSPAs would then help address the gap between the law and technology. Keeping MAPs current would show how the students could work toward real issues and adjust as companies seek new and current talents. MAPs would not be vocational nor prescriptive guarantee for job placement. However, the MAPs would show how the educational institutions are tuning the courses, content, and instructors to meet metrics for matriculations, rising stars with strategic companies for building institutional reputations, and doing relevant technical research.

My brief bio:

Published in IEEE and certified as a PMP, Mr. Hon proactively helps Federal clients with challenging projects and vendor management issues in Cyber Security, Cloud Computing, and Foreign Assistance areas for over 20 years. As a CISSP, Mr. Hon has also taught Cyber hacking and other technology courses for 17 years. He has spoken internationally and at numerous law enforcement

Thank you for your consideration!

Mun-Wai Hon, CISSP
MHon@nvcc.edu

Cybersecurity Education for Children of the Information Age

Cynthia Irvine

Naval Postgraduate School

April 2018

1. Problem Statement

A number of excellent programs have been developed to introduce K-12 students to cybersecurity. Examples include presentations by industry and academic experts; multi-day camps and gatherings featuring cybersecurity as a theme; and cybersecurity awareness days, weeks, or months that may involve discussions of cybersecurity and hands-on activities illustrating cybersecurity concepts and problems. Such activities can generate high levels of student interest in cybersecurity. They share two common characteristics.

First, these activities are discontinuous. Short intervals of high intensity learning may be followed by long periods during which student enthusiasm dwindles. Even with take-home materials, students may be set adrift. Without reinforcement, few students will progress between events. At the next event, students may be familiar with various topics but, with minimal advancement in the interim. To progress, students need practical tools for learning about cybersecurity, as well as help and encouragement from parents and teachers.

Second, short programs require the presence and deep involvement of cybersecurity experts. The paucity of such experts limits short programs in terms of their duration and participant numbers. Furthermore, there are far too few cybersecurity experts to provide on-location support to school districts nation-wide.

The relatively small number of students involved in short-duration programs is a serious issue. Mechanisms are needed so that substantially larger student populations have access to computing and cybersecurity education. These mechanisms must be formulated so that they can succeed in resource constrained contexts.

Parents can review the homework assignments and help children with reading, spelling, and standard arithmetic and mathematics. Similarly, teachers know how to present these materials in the classroom. Yet today, parents and educators are ill equipped to help children learn about computing and cybersecurity. Some may not even believe that these topics can be taught to their children.

Just as there are programs that encourage parents to read to their children, educational programs are needed to enable typical teachers and parents to help the children of the information age learn about computing and cybersecurity.

2. Idea: A Multi-pronged Approach

Public Appreciation

Greater public appreciation of the "wonders" of computing and cybersecurity is needed.

How can parents and teachers support their children and students if they know **nothing** about how computers work? They do know that computers are part of daily life. From smartphones to grocery store checkouts and utility meters, they know that computers are at work, but they don't know how. They may also be aware that cybersecurity is a problem. Yet most people have no idea of the true extent and vulnerability of the computing ecosystem. Cyberspace appears far too complicated and difficult to understand.

Why should this be so? Millions of non-scientists appreciate the wonders of the universe. They support space research and NASA programs. Similarly they appreciate the elegance of a well engineered car. They may know more about Stephen Hawking and concept cars than they do about how they are connected to their local ISP. Public education programs are needed so that citizens can appreciate the achievements and challenges associated with building and operating cyberspace. They can also be made aware of the opportunities and rewards associated with careers in cybersecurity. Such appreciation will not turn everyone into a computer or cybersecurity expert, but it will help parents, teachers, and others encourage young people to learn about and enter these fields.

An Environment for Ongoing Computing and Cybersecurity Education

To build and maintain student interest in computing, an environment that supports computing and cybersecurity tools and exercises should be available year-round. The environment should:

- Present low barriers to participation.
  - Be easy for typical teachers to use.
  - Its per-pupil cost must be low.

- Engage students and allow them to build and explore. It should be designed to encourage students to experiment and learn, not race to the finish.
- Allow students to progress at their own rate, while helping all students achieve a sense of self efficacy.
- Individualize student work. No copying from someone else!
- Allow disinterested students to quit (after mastering some minimum set of knowledge). Not everyone needs to play the clarinet, neither must everyone become a cybersecurity expert.
- Assist educators with routine grading tasks.
- Ensure that each student's performance and progress can be measured.
- Identify students needing assistance, and permit reenforcement of their basic knowledge and skills before moving them to more difficult concepts and tasks.
- Allow parents to appreciate student progress (see below).

Objectives for the overall environment might include:

- Respect privacy.
- Support statistical analysis of ongoing results. For example, it may be desirable to understand how the environment works for different social and economic populations.
- Design for rapid extension and adaptation. It should be possible to roll out new versions of the tools relatively quickly.
- Allow alignment with the cognitive development of students. Measures of student readiness in terms of information processing, abstract reasoning, etc. for certain topics would be useful. This would prevent frustration for for both rapid and evolving learners.
- Reward persistence, not competition.

Ultimately, high aptitude students can be identified and encouraged to pursue advanced cybersecurity studies. Students with other goals will benefit from an appreciation of how computing and cybersecurity work and will be better cyberspace citizens.

Companion Tools for Parents and Educators

Easy to use tools should be developed to allow parents and teachers new to computing and cybersecurity to support and follow student progress. Student homework tasks should be designed so that parents can know that children are completing their assignments, despite not understanding the details of those assignments. However, it should be possible for parents to learn along with their children. Individualization of assignments can ensure that parents-as-learners are not doing their children's homework for them. Similarly, tools can be constructed so that teachers could learn along with their students.

A benefit to having parents and teachers learn in parallel with students is that some may find that they have the aptitude and proficiency to pursue professions in computing and cybersecurity. If structured properly, these individuals could continue their studies in post-secondary education programs.

Use Cybersecurity Experts Wisely

Computing and cybersecurity experts will be needed in all facets of this effort. Public appreciation of cyberspace and cybersecurity will require translation of technical topics to the general public. Everyone needs to have some understanding of how cyberspace intersects with and affects the physical world. Lessons and tools will need to be designed to cover not only how computers and cyberspace constructs are built and operate, but to address a plethora of social, legal and ethical issues. Mechanisms to ask for and receive help with aspects of the environment will needed.

Closing Note

Although this paper focuses on K-12 students, many of the concepts associated with the proposed environment could be applied to post-secondary education in cybersecurity, both traditional or nontraditional.

New Approaches to Cyber Education (NACE) Workshop

Educate the Educators to Equip the Next Generation

By: Joni L. Jones Associate Professor Information Systems and Decision Sciences, Muma College of Business, University of South Florida

When considering the education needed to equip the next generation to become cybersecurity and privacy specialist we need to address who to educate, what to teach, and how to sustain the pipeline. Cybersecurity is a rapidly evolving arena of topics and mindsets. We need to concentrate our efforts in creating students that can think and react to this environment. In order to make our efforts fruitful we need to start in K-12 where we have the largest potential candidate pool and most malleable minds. Two main focuses are a basic understanding of technological topics. Essential core technology skills include programming and computer literacy, networking and internet connectivity, big data/data privacy and ethical issues exacerbated by the ubiquitous nature of technology. More importantly, students need to be comfortable with experimentation and experiential learning. In this fast paced milieu students and eventual practitioners must be self-motivated problem solvers that question norms, propose inventive solutions and out think the cybercriminal. As university academics we need to focus our efforts on preparing instructors with the necessary skills to make this happen. Our focus should be on training the trainers.

The question then becomes how do we create such students? Much of our current education is based on route memorization and lecture. Moving toward a more experiential learning experience is imperative to engender the skills needed for successful cybersecurity and privacy specialists. Therefore, the first task should be to educate the educators. According to the State of the States Report: State-Level Policies Supporting Equitable K-12 Computer Science Education (2017) "There are simply not enough adequately trained people to full the current need for information security analysts, hardware engineers, software developers, computer programmers, data scientists, and other STEM professionals (pg. 7, Stanton, et al. 2017)." For example, according to Code.org, only 241 schools in FL (22% of FL schools with AP programs) offered an AP Computer Science course in 2016-2017 (13% offered AP CS A and 16% offered AP CSP), which is 95 more than the previous year. There are fewer AP exams taken in computer

science than in any other STEM subject area. Additionally, Florida universities did not graduate a single new teacher prepared to teach computer science in 2016. This deficit indicates an area where assistance is needed in the form of tools and experiential learning materials and environments that are easily deployed by all faculty. These experiential learning materials could include project or game based lessons such as capture the flag, hackathon, or team competitions. Cyber ranges and other technical playgrounds are essential to facilitate these type of experiences in contained and safe settings. With these type of educational tools you are also advancing problem solving skill building. Organizations similar to DECA (Distributed Education Clubs of America) and the Whitehatters should be recruited to develop and hold national competitions to act as a resource, outlet, and incentive.

Another major motivator to attract and educate a diverse set of students to succeed in a variety of national and private sector positions is to ensure that students know the career paths an opportunities available to them. Increasing the visibility of positions, the skills required, salary ranges, daily activities, etc. will allow students to visualize themselves in the career path and drive enrollments. Not every student may choose a traditional 4-year university degree so there needs to be a variety of paths to acquire the necessary skills. These paths could include vocational training, community college, as well as the traditional 4 year university degree. All should employ High Impact Practices (HIP), namely, internship opportunities to gain hands on experience. Unfortunately, in the area of cybersecurity this can be difficult due to security issues with organizations. Alternatively, other HIP experiences could include case based learning, capstone courses or other settings that pose situational conditions to students that require problem solving and an opportunity to apply their learning via a culminating assignment.

To ensure that the education we provide is consistent and executable requires a concerted centralized structure of support. A centralized body would need to be responsible for establishing standards and curricula, promoting best practices, providing continuing education, and accreditation. They can also participate in the creation and hosting of national and international competitions and/or establish a national student organization.

While cybersecurity education cannot be expected to train for every platform it is imperative that academia and industry form partnerships. These partnerships should include externships for faculty to work with industry to develop curriculum and gain valuable field experience. To enable hands on training industry can collaborate with higher education to create environments, cyber ranges and other training materials to enhance student engagement and practical skill development. Corporations and cyber application developers are uniquely positioned to supply expertise and fund/donate technology. Academia can then generate, possibly in partnership with industry, lessons and curricula that utilizes the corporate supplied technology and use cases.

In summary, to ensure that we keep pace with the ever-changing and rapidly growing need for a cyber-ready workforce we need to work collaboratively with K-12, industry, and upper level academia. This public-private partnership will blend classroom learning with workplace experiences. We need to train the trainers on technologies and cyber trends to facilitate this learning. More importantly, we need to expand and facilitate experiential learning to promote student's problem solving skills, encourage persistence and integrate their knowledge into a contextualized experiences.

References

Stanton, J., et al. 2017, State of the States Report: State-Level Policies Supporting Equitable K-12 Computer Science Education (2017) Retrieved from http://www.edc.org/sites/default/files/uploads/State-States-Landscape-Report.pdf

Schaffhauser, D. (2017) State Progress on K-12 Computer Science Ed Policies: 'We Have a Long Way to Go' *THE Journal – Transforming Education through Technology (04/10/2017)* Retrieved from https://thejournal.com/articles/2017/04/10/state-progress-on-k12-computer-science-ed-policies.aspx

K12 Computer Science Framework (2016). Retrieved from http://www.k12cs.org

BIO

Joni Jones is an Associate Professor in the Information Systems Decision Sciences Department and Academic Liaison for the MS Cybersecurity Degree Prohgrams. She teaches various graduate and undergraduate courses including global cyber ethics, decision analysis for business

continuity and disaster recovery, systems analysis and design, business honors professional development, and research methods. She previously taught introductory courses in computing as well as courses in C#, managerial statistics, business system application and design, and software applications.

Her research interests include electronic commerce, pricing models for information goods, information and prediction markets, social networking and cyber ethics. Her research has been published in the MIS Quarterly, Production and Operations Management, the Journal of E-Commerce, INFORMS Journal on Computing, Decision Support Systems and presented at national and international conferences.

Jones holds a BS in business administration from the University of Illinois, Chicago, and earned a PhD from the University of Florida. She joined USF in 2003, having previously taught at the University of Michigan, the University of Florida, and Santa Fe Community College. Her professional service includes roles as a reviewer for numerous academic journals. She is a member of Beta Gamma Sigma.

A Cyber Security Library – The need, the distinctions, and some open questions

Sidd Kaza, Department of Computer and Information Sciences, Towson University,
skaza@towson.edu

It is clear that in order to address the cybersecurity education and workforce crisis, the challenges are not just numerous but also inextricably linked. The least of which include a greater number of prepared faculty, effective curriculum, and infrastructure to host, use, and disseminate the curriculum. There is a demonstrated need for a cybersecurity digital library (DL) that will help address these challenges. The Cyber DL is similar to other curricular digital libraries in some respects (material quality, uptake, etc.) and unique in others (national security concerns, presence of damaging material – malware, material integrity issues, etc.). This idea paper articulates the need, the similarities, the distinctions and open questions, and provides some insights based on an ongoing Cyber DL project.

A Cybersecurity Digital Library – The need

Perhaps the greatest challenge to a successful digital library is the buy-in of the community behind it. For a cybersecurity digital library, this community includes academicians, industry, government standards and designation bodies, and the students who need the effective curriculum to contribute to our nation's workforce. Academia has taken advantage of the funding available from the National Science Foundation, National Security Agency, Department of Homeland Security, and other funding agencies available in the cybersecurity education arena. We have clearly reached a tipping point where there is effective curriculum to be had, only if there was a place to find it. There are early innovators responding to the need for curriculum sharing in cybersecurity education, such as CyberWatch, Department of Homeland Security (DHS), and SkillsCommons.org. There are similar efforts in computer science such as Ensemble, EngageCSEdu, NCWIT and in other STEM fields as well. The existing repositories offer several good features and a solid base on which to build, but there are several issues that need to be considered in the five-year horizon for a cybersecurity digital library to succeed.

A Cybersecurity Digital Library – learning from others

Vannevar Bush suggested the use of computers to retrieve information in 1945 (Bush 1945). The most recent surge in the term "digital library" came with the National Science Foundation funding research in the area through the Digital Library Initiatives through the nineties and into this century. There is a much cited formal framework focused on Streams, Structures, Spaces, Scenarios, and Societies to define digital libraries rigorously (Gonçalves et al. 2004) - Streams are sequences of items that describe static and dynamic library content. Structures are labeled directed graphs, that impose organization. Spaces are sets with set operations that obey certain constraints. Scenarios consist of sequences of events that modify states of a computation in order to accomplish a functional requirement. Societies are sets of entities and activities and the relationships among them.

A successful Cybersecurity Digital Library effort, has much to learn from the DL literature on what makes a "good digital library." There can be several quality indicators of the digital objects, metadata, collections, catalog, and services for a digital library. These include (Goncalves et al. 2007) accessibility, accuracy, completeness, composability, conformance, consistency, effectiveness, efficiency, extensibility, pertinence, preservability, relevance, reliability, reusability, significance, similarity, and timeliness. This is a rather long laundry list of quality indicators, and each is accompanied by metrics to measure them. As we build a Cyber DL, we will need to interpret and apply each of these to the new digital library.

A Cybersecurity Digital Library – Distinctions

There are several unique aspects and challenges to a Cyber DL that have not been explored in the digital library literature. In our work in building a prototype Cyber DL (www.clark.center) and working with the community, and beta-testers, we have identified the following issues (technical, policy, and social) that highlight the distinctions.

Complicated security policies – A Cyber DL will likely store cybersecurity curriculum that might provide the knowledge needed to cause malicious damage. One might argue, that such

knowledge is found quite easily at other places on the web. However, this curriculum might be accompanied by pieces of Malware that will be used in sandboxed environments in the classroom (a rather common practice in security courses). Security policies need to be implemented to host, distribute, and sandbox this Malware. How do we ensure that an open Cyber DL does not become a "Dropbox" for Malware? How do we ensure that only qualified faculty have access to the materials?

Disclaimers and protection – Closely related with the previous policy issue, is the protection that a Cyber DL will need to have from potential damage the distributed content might cause. Does there need to be protection for the host – whether it be a university, a non-profit, or a private company?

Attacks from adversaries – As with any large-scale web application, security and availability would be a concern for the Cyber DL. However, producing cybersecurity professionals also contributes to our national security. Would a national Cyber DL become a soft target, needlessly attracting attention as it hosts curriculum that our CAE and other institutions use? If this indeed is an issue, what protocols and resources need to be in place to mitigate this risk and are they any different from other digital libraries?

Faculty incentives – Cybersecurity curriculum is challenging to build, deploy, and update. Though other disciplines might be similar, we can contend that cybersecurity learning materials will need to be updated more frequently and will require a dissemination plan so content consumers are not just notified but also involved in the maintenance of materials. If that is the case, the Cyber DL needs to include an incentive plan for content creators. Maybe a music subscription like plan ("the artist gets a small cut for each download") or maybe a 'tipping' system (recommended at a recent workshop). In the age of Kickstarter, is a crowdsourced sustained funding source the way to go?

Storage, licensing, and dissemination – Several cybersecurity materials come with virtual machine (VM) environments that cater to the learning objects. Even with the seemingly endless storage capacity and bandwidth that we appear to have available, distributing VMs becomes a problem that scales very quickly. Cyber DL solutions will need to look at creative ways to not just store, but create a versioning for VM images, look at software licensing issues (and not become a "Dropbox" for pirated software), and look at bandwidth scaling very carefully so frivolous multiple downloads do not lead to escalating hosting costs. Should the Cyber DL consider partnering with a Cyber Range (Dark et al., n.d.) or maybe partner with a corporation (like Google) to donate storage and bandwidth?

The challenges in building a Cyber DL are many, but a discussion to answer some open questions will go a long way in making this digital library successful.

Acknowledgements

At Towson University, we are working on a pilot for a Cybersecurity Digital Library called CLARK (Cybersecurity Labs and Resources Knowledge-base, www.clark.center). CLARK is supported by the National Security Agency under NSA Grant H9830-17-1-0405. Though the language in this idea paper is the author's, some of the ideas are shared with Melissa Dark and Blair Taylor in their capacities with the NSA College of Cyber. To remove conflict of interest, neither Dark or Taylor reviewed this paper prior to submission.

References

Bush, V. 1945. “As We May Think.” *The Atlantic Monthly*, 1945.

Dark, M., S. Kaza, S. LaFountain, and Blair Taylor. n.d. “The Cyber Cube: A Multifaceted Approach for a Living Cybersecurity Curriculum Library.” In *The Colloquium for Information Systems Security Education (CISSE)*. New Orleans, LA.

Gonçalves, Marcos André, Edward A. Fox, Layne T. Watson, and Neill A. Kipp. 2004. “Streams, Structures, Spaces, Scenarios, Societies (5s).” *ACM Transactions on Information Systems* 22 (2). ACM: 270–312. https://doi.org/10.1145/984321.984325.

Goncalves, Marcos Andre, Barbara L Moreira, Edward A Fox, and Layne T Watson. 2007. “‘What Is a Good Digital Library?’ A Quality Model for Digital Libraries.” *Information Processing & Management* 43 (5): 1416–37. https://doi.org/10.1016/j.ipm.2006.11.010.

Author Bio

Dr. Sidd Kaza is the Chairperson and Associate Professor in the Computer and Information Sciences department at Towson University. He received his Ph.D. degree in Management Information Systems from the University of Arizona. His interests lie in cybersecurity education, data mining, and application development and he is a principal investigator on several cybersecurity education projects. He is also on the ACM Joint Task Force on Cybersecurity Education and is the recipient of the University System of Maryland Regent's Award for Excellent in Teaching. Dr. Kaza's work has been published in top-tier journals and has been funded by the National Science Foundation, National Security Agency, Department of Defense, Intel, and the Maryland Higher Education Commission.

New Approaches to Cybersecurity Education: CTF 101 Elective

Rana Khalil
University of Ottawa
https://rkhal101.github.io/

1. Introduction

Despite being one of the fastest growing fields, it is estimated that there will be 3.5 million unfilled cybersecurity positions by 2021 according to a recent report by Cybersecurity Ventures [1]. The reasons behind this cybersecurity labour crises are many, however one of the significant contributing factors is the lack of cybersecurity knowledge and skills. Individuals who obtain their degrees in areas such as computer science have a weak foundation in security principals. The approach used to introduce students to computer security usually involves either only introducing security in upper level courses or integrating security into the curriculum by quickly brushing over the theory behind the related security concepts with little to no practical exercises. In both cases, the students of such institutions graduate without a solid foundation in the basic computer security concepts. Introducing security across the curriculum through practical exercises is not a new concept and has been suggested by academia over and over again [2] [3]. Although the approach taken by institutions to implement this change has been lacking and many improvements can be suggested, this is not the focus of this proposal.

This proposal is inspired by an elective mathematics course implemented by the University of Ottawa in order to introduce students to the field of statistics and probability. The course is called Poker 101 [4] and was introduced as a creative way to teach students across all faculties about core concepts in probability and statistics. The course was first offered in 2011, and although it was offered as an elective, students from several faculties registered and successfully completed the course [5]. Using this innovative approach to teach probability and statistics, this proposal suggests the implementation of a course teaching the core concepts of computer security using the methods in capture the flag security competitions.

2. Capture the Flag 101 Course

The idea is simple. Capture the flag security competitions are known to be attended by individuals from diverse academic backgrounds. Due to the lack of security education in non-cybersecurity degrees such as computer science and software engineering, these individuals are also usually self-taught. However, due to the nature of capture the flag competitions where participants are given exercises to complete with little to no information or prior training on how to approach these exercises, many promising individuals might shy away from participating in such competitions, especially individuals that belong to minority groups. As a result, such individuals miss out on a great opportunity to learn and practice the security skills that the industry is in desperate need of.

This report proposes the implementation of an elective course that teaches the core concepts and skill sets required to participate and complete capture the flag competitions. This would include topics such as forensics, cryptography, web exploitation, reverse engineering and binary exploitation. The concepts would be introduced and taught to the students with the tools necessary to understand these concepts. Then students are presented with challenges to apply these concepts.

An implementation of such a course, especially at an early stage of a degree, will inspire students to pursue a career in cybersecurity or at the very least compel these students to be more security aware when taking other courses in their degrees. Another direct benefit of such a course is that students will be more encouraged to participate in CTF competitions and therefore further their skill set.

3. Conclusion

This report proposes the implementation on an elective course that teaches the core computer security concepts in the style of a capture the flag competition. This was inspired by a successful mathematics course introduced by the University of Ottawa, called Poker 101, that introduced the core concepts in the field of probability and statistics. Offering such a course can inspire students to pursue a career in cybersecurity and make students more security aware in the degrees they pursue. Implementation of such a course is very feasible and is likely to be successful considering the significant interest in CTF competitions from individuals pursuing both cybersecurity and non-cybersecurity degrees.

References

[1] Cybersecurity Jobs Report 2018-2021. https://cybersecurityventures.com/jobs/, Last accessed: 2018-04-30.

[2] Major Gregory White. Security across the Curriculum: Using Computer Security to Teach Computer Science Principles. 1996.

[3] W. Dwayne Collins. Introducing Computer Security Concepts in Introductory Computer Science Courses. J. Comput. Sci. Coll., 20(6):41–47, June 2005.

[4] Probability and Games of Chance! Poker 101. http://mysite.science.uottawa.ca/phofstra/MAT1374/index.html, Last accessed: 2018-04-30.

[5] Using math to beat the odds. https://www.uottawa.ca/gazette/en/news/usingmathbeatodds, Last accessed: 2018-04-30.

Author's Biography

Rana obtained her Bachelor of Computer Science and Mathematics at the University of Ottawa and is currently pursuing her Master of Computer Science with a focus on open source web application vulnerability scanners. During her time at university, Rana took upon herself various volunteer and leadership roles which included University of Ottawa ambassador for Seeds for the Future Huawei Canada, Orphan Sponsorship Initiative Vice Chair, Women Startup Network Peer Mentor, IEEE University of Ottawa Student Branch VP Academic and IEEE University of Ottawa Student Branch Women in Engineering Vice Chair.

Rana has worn many hats during her work in the public and private sector. She held positions as a spectrum engineer assistant, automated tester, software developer, security analyst and as a ransomware researcher. Rana currently works at the University of Ottawa as a Teaching Assistant for several second and third year Computer Science courses. As a teaching assistant, Rana teaches weekly lab/tutorial sessions, holds weekly office hours, marks theory and programming assignments and proctors midterms and final exams.

Rana is deeply passionate about her degree in computer science with a deep interest in computer security and is determined to make a difference using the degree she is pursuing.

Integrating Ethics in Cybersecurity Education

Mohammad Taha Khan, Chris Kanich and Cynthia Taylor
University of Illinois at Chicago and Oberlin College
{mkhan228, ckanich}@uic.edu, cynthia.taylor@oberlin.edu

Introduction

Ethics plays a critical role in cybersecurity and provides the moral distinction between black-hat hackers and cybersecurity professionals. The study of ethics in cybersecurity is a complex matter, and as the need for security professionals grows, educators and employers alike have focused more on raw numbers and technical competency than on ensuring that these professionals understand the ethical underpinnings of their sensitive and important roles within any given organization. Whether dealing with entrusted personal user data, developing a framework to store passwords, or investigating a data breach, all such tasks must be executed ethically which requires training beyond the technical aspects of cybersecurity.

Ethics has long been considered important to Computer Science in general, with the ACM and IEEE model curriculums both including it, and ABET requiring coverage of ethics for accreditation. In 2006 Quinn [1] showed that fifty-five percent of ABET accredited CS departments teach computer science students about ethics through a dedicated course on the social and ethical implications of computing, and argued for the benefits of offering ethics courses taught by Computer Science professors. As cybersecurity itself becomes a highly specialized and in-demand branch of computer science, its adversarial, mission critical role coupled with stewardship over an organization's critical infrastructure and private data necessitates a more specialized ethics curriculum tightly integrated into security-related courses.

Here we outline how to improve the overall instruction of computer science ethics by refining the content of the sole ethics course offered for computer science majors and by

integrating ethics into computer science courses. In addition, we suggest pointers which can be useful in training students from diverse backgrounds for practical situations.

We believe that teaching ethics as an integral component of cybersecurity education will empower future individuals to act responsibly when dealing with sensitive data. These suggestions will also help them better understand the irreversible implications of data breaches and hence promote the adoption of more secure and correct programming practices. Finally, a part of this ethics training, students will also learn how to carry out due diligence in situations of cyber attacks and breaches. The next sections provides details of our proposed ideas.

Suggested Approaches

Teaching The Ethics of Privacy Through Personalized Experiences: Ethics and privacy go hand in hand and a lot of components of ethics for cybersecurity revolve around safeguarding privacy. While the notion of privacy is extensively covered in the traditional computer science ethics course, the descriptions and examples can sometimes be too broad and hence result in a disconnect of the students understanding of privacy in context and it can be hard for individuals to understand the gravity of personal information leakage. However, all college students have personal experience with making their own data available in varying degrees online. By having students take surveys on how they currently share data or discuss the ramifications of having their data made public in various hypothetical situations, instructors can explain the ramifications of privacy policies in a realistic, student-centered way. It is also important that instructors discuss that the ramifications of data becoming public will vary greatly depending on the individual: for example, past dating profiles becoming public may have a very different implication for someone who is gay than for someone who is straight. These activities need to be designed in a meticulous and fine grained manner and require the involvement and overlapping interaction of ethicists and cyber security professionals to sketch out an accurate design.

Including Ethics Components Within Cybersecurity Courses: When ethics is included in the CS curriculum, it is usually taught as a separate course. Even when it is a required course for graduation, it is frequently seen by students as an "easy A" course, and less important than more technical courses. This, combined with the abstract nature of the course frequently results in students not taking much interest, and failing to develop the full practical context of ethics and its importance. Given the importance of ethics to cybersecurity, it's important to add ethics to security courses themselves, as well as covering cybersecurity topics in general ethics courses. This should be done by the including both case studies as well as collaborative exercises. Students should be provided case study readings that pertain to the technical material being covered in class. For instance, while teaching them about SSL and secure web applications, students should have readings about how the Heartbleed bug was committed to the OpenSSL and how it went undetected for years and had catastrophic implications.

Another example of having a more involved activity on ethics can be having students perform an SQL injection (as a part of their assignment) on a sample healthcare database. For submitting solutions, apart from providing malformed queries, students should be asked about their perceptions on how they felt about the data leaked and what possible implications it could have. This will not only allow them to learn the importance of dealing with sensitive data but also provide implicit feedback to the instructor to better evaluate the understanding and perceptions of ethics.

This supplementary approach to teaching ethics will not only strengthen the principles of the students, but will also provide them with real-world examples and implications, which will encourage better programming practices and enable them to realize how as cybersecurity professionals, their design decisions can impact millions of individuals.

Acquiring Industry Feedback: Finally, we also suggest that gaining feedback from senior level cyber security professionals can also helpful and can help develop a more practical curriculum. This can be done in the form of meetings, surveys as well as workshop or panel based interaction where educators can get real insights on what are

the main elements and components of ethics that should be focused on within the courses.

Ethics Within Graduate Security Courses: While the major proposed focus of this idea paper revolves around improving the ethical standards of undergraduate cybersecurity courses, at the same time, it's an important to realize that there should also be continued ethical training for graduate students. This is especially important as students without a US-based undergraduate education are less likely to have been exposed to ethics courses as part of their undergraduate education. Just as students are exposed to more complex computer science problems as graduate students, they should likewise be exposed to more complex and nuanced ethical issues.

Conclusion

Overall, we believe that a more integrated ethical framework is the right step forward in the direction of educating the cybersecurity professionals of tomorrow and will likely avoid situations like the Target breach or Cambridge Analytica. It is our hope that coupling ethics with mainstream technical education will result in better trained cybersecurity professionals.

References

[1] Quinn, Michael J. "On teaching computer ethics within a computer science department." Science and Engineering Ethics 12.2 (2006): 335-343.

Authors Bio

Mohammad Taha Khan is a 4th year PhD student at the University of Illinois at Chicago. His research interests span the domain of security and privacy on the Internet. His focus is on understanding privacy leakage on the Internet, socio-technical aspects of cybercrime and human factors in security. As a lot of his work incorporates insights from empirical analysis, he is particularly interested in developing better teaching methodologies around the ethics of data collection and management. After graduation, Taha plans to pursue teaching based academia.

Chris Kanich is an Assistant Professor at the University of Illinois at Chicago. He conducts research on the socio-technical aspects of cybersecurity. His current work includes analysis of gains and losses due to undesirable activity on the Internet, investigating human factors in effective Internet security mechanisms, and building new technological primitives with the goal of increasing the practical security and privacy of Internet users.

Cynthia Taylor is an Assistant Professor at Oberlin College. Her research interests include Security and Computer Science Education. Her education research interests include active learning, with a focus on peer instruction, and assessment of student learning via concept inventories. Her security research looks at how people use the internet, and its implications for security.

Denise Kinsey

Submission #1 nace@cerias.purdue.edu

Proposal paper in support of 'shared' cybersecurity special topics course.

While it supports many of the ideas presented in the CFP, this paper offers an approach that specifically addresses these questions:

- What skills and knowledge should people in the field have, and how should that be acquired?
- How do we get more US citizens—and a more diverse population —into cybersecurity in meaningful ways?
- What kinds of resources and materials for use in education and training are needed, how do we get them developed, and how do we measure their effectiveness?
- What are some good ways to "future-proof" the education we provide?

One issue plaguing academia is the need for timely information and training yet by the time a 'new' or cutting edge course is created it is outdated and in need of a refresh. While adding current events helps it does not address the fact that faculty can't be experts in everything or hold experience and credentials to teach every topic encompassed in 'cybersecurity', which means each term only a select few are fortunate enough to attend classes by experts in cybersecurity niche topic areas.

I propose that an emerging technology course is created, but instead of teaching or training a few teachers how to replicate the material, which is quickly outdated and for which they may not hold the necessary expertise, that the program recognize the experts in those areas and synergize the classroom by offering that special topic course on emerging technologies to other schools at the same time through a webcast format. Attendees would need the same level of pre-requisite skills, but this proposal extends teaching specialty topics to a few faculty to instead teaching many classes across the country at the same time each semester.

This proposal allows for recognition of cybersecurity experts while extending the reach of their expertise from a handful of teachers to many students across the country (or online if deployed military, etc) to allow them to gain knowledge in these emerging or niche topic areas where we have a pronounced need. It eliminates the need for schools to be seen as competitors and instead as compliments as competing programs and duplication of expensive resource labs may become a thing of the past.

How would such a proposal work? The teacher of record at each school is still responsible for their class in whatever format it is offered. The web hosted teacher can do this in conjunction with teaching their own classes of the same topic at the same time. The teacher presenting the material (web host/remote teacher) would create some resources for the remote on- ground faculty including a detailed rubric for each assignment, prerequisite readings, etc. to ensure that the students watching at a distance have the ability to understand the material and their teacher has the information to properly score the assessments.

The class would be taught by a combination with the expert in a web-format/webinar so the expert may broadcast from their home school/lab and all participating schools may benefit. This highlights the expert and allows all to benefit from that expertise, and it allows for schools to specialize in certain areas while still offering additional electives and specializations that otherwise would not be options for that student population. To accomplish this, the expert teacher who broadcasts the material will receive an additional stipend and the teacher of record from participating schools will still be paid as the local teacher as this person needs to grade, interact, answer questions, and facilitate the learning process. This type of cross-school and cross-class partnership has many benefits as all who participate are paid, the skills of the expert are shared to a broader audience, it reduces unnecessary or inferior replication of course topics, offers an audience to non-traditional applications or specializations in cybersecurity, and extends the reach of necessary course content beyond traditional classroom borders.

The webinar should be an interactive session allowing the on-ground faculty in each class to gather questions and assist their class. The on-ground teacher can augment the material with

additional items to aid in understanding or make it more relevant to the participating population. These items can include current events, grading course projects and research, guest speakers from industry and government, application of how the content applies to cybersecurity compliance, regulation, and governance.

The teacher hosting the webcast class would receive a stipend for the course materials and remotely teaching the sessions (for all class periods or a pre-determined number of times within a course to demonstrate the most difficult topics or concepts the remote school can't supply (such as those needing a specific lab set-up to allow for successful demonstration)), and for assisting local faculty in teaching and challenging their population of students.

The web portion should not be used as a recording to replace teachers, but should only be used in the event of class cancellation, to facilitate review in remote areas (such as military students deployed in drastically different time zones which would prohibit real-time attendance at the webcast, or daytime courses when the expert only teaches in the evenings for example) or to allow for review and remediation of the material. To keep the content fresh and to compensate the remote teacher for their effort and expertise, live webcasts should be performed.

This proposal addresses the need for flexibility in cybersecurity curriculum to address emerging topic areas, matching newer faculty or those untrained or lacking experience in an area of cybersecurity which is essential to student success in the workforce, and removes the financial barrier to many schools offering timely and necessary cybersecurity subjects, while showcasing the excellence held by some institutions in various cybersecurity areas. This is a concept that would require trust by both schools and the involved faculty, but which may ultimately solve some of the issues faced by our present lack of capacity to meet the needs of business and industry, resulting in our shortage of well-trained and educated cybersecurity workforce. Opening up the expertise in some of the topic areas may inspire greater enrollment by women and minorities as they would have access to these niche classes at their local college. It also offers the opportunity to showcase experts who may be women and minorities to areas of the country that have a less diverse faculty. Finally, this concept meets the CAE/CAE2Y requirement of shared teaching and resources.

The created material would become part of the collection made available to the CAE community – maybe hosted by CyberWatch or CSSIA in their curriculum repositories for designated schools to use. This could be limited to CAE/CAE2Y schools as a means of validating the pre-requisite and foundational skills and as an added benefit of becoming a CAE.

Denise Kinsey

Submission #2 nace@cerias.purdue.edu

Proposal paper in support of uniquely crafted externships/course projects.

As with proposal paper #1, this proposal supports many of the ideas presented in the CFP and specifically addresses these questions:

- What skills and knowledge should people in the field have, and how should that be acquired?
- How do we get more US citizens—and a more diverse population —into cybersecurity in meaningful ways?
- What kinds of resources and materials for use in education and training are needed, how do we get them developed, and how do we measure their effectiveness?
- What are some good ways to "future-proof" the education we provide?

One area lacking significantly in cybersecurity education is hands-on experience that aids in student learning and which can be listed on student resumes. In academia, most learning is passive which makes recall and complete understanding of a subject more difficult. This results in a shortage of well-educated and trained workers in cybersecurity. Students learn best and have a means to 'relive' the experiences through relevant, hands-on learning. One way to help students understand the cybersecurity job environment, and therefore provide a better assessment of understanding than traditional lecture courses, is to provide an immersive experience through in-depth, real world projects. Presently, most cybersecurity topics are presented as silos and not infused into other disciplines or even shown as a compliment to other IT and cybersecurity content areas. Learning requires context and a base of knowledge to best apply those concepts to situations, resulting in students synthesizing ideas to create solutions, just like what is expected when students are on the job.

To solve this problem we could include hands-on projects from the community and partner on-ground courses with online courses/schools to expose more students to these opportunities.

Those on-ground would perform the actual tasks while those participating remotely will offer consultative services. In an entirely online situation students could complete projects remotely including researching a problem and offering the best solution, with security infused into the solution design. Actual implementation may be left to the company or an on-ground class.

While ambitious, this idea can work. My courses and students are proof of its success. I have been the teacher for on-ground and online students as we completed over 115 IT and cybersecurity projects for nonprofits in Ohio, Indiana and Texas. While my on-ground students did the bulk of hands-on work, my online students offered design and troubleshooting assistance and participated from different states, countries, some while serving in the military in places like Kabul, Japan, Germany, and two were on nuclear submarines! This idea works. We even completed a project for a battered woman's shelter where the women had to perform the work and the men had to act as consultants as no men were allowed onsite.

So far, all of the work has been completed by my students while I worked for multiple educational institutions. The on-ground students usually consist of a single class for a single school but have included several online students who either lived nearby or were able to travel to the location. The remote assistance in the form of research, troubleshooting, code/plan review were often from different schools where I taught online and participated as volunteers instead of a designated course project.

This semester I had a student participate who was enrolled at a school where I do not teach as he was the significant other of a current student and he was able to provide a level of expertise the class did not possess. The team he worked with was grateful for his assistance and experience and the project progressed faster than anticipated because of it.

The application of this proposal could result in two potential applications of this concept: 1) Train teachers to facilitate their own outreach and inclusion of hands-on community projects for their online and/or on-ground classes, and; 2) Partner teachers who are online with teachers willing to participate on-ground to benefit communities, open opportunities for experience and volunteerism to their students, and offer project-based learning activities which are much more authentic and realistic than many traditional projects and research papers.

Obviously, option 1) empowers teachers to facilitate the process independently while option 2) would require a bit more coordination between faculty and partnering institutions, but I promise it is worth it!

Often, we begin the volunteer work with a risk assessment which provides the organization with the knowledge of what is needed to protect people, property, and processes. Completed projects have included planning, designing, and building networks (usually with equipment supplied by the organization, but a few times we refurbished equipment or raised money to purchase the equipment), operating system security, secure development of middleware, website development and implementation, network/application/wireless troubleshooting, funding integration (ability to accept donations), and many others.

Not every project requires a site visit. For example, this semester in my secure development course we worked on development of two websites, a mobile application, middleware for a dentist's office, and a new distribution of Linux. Some of those were real non-profit projects and others were of my creation but which could be marketed – such as the mobile application which could be sold (low cost) in the app store with all proceeds going to the cybersecurity club, and the Linux distribution would include the names of all participants as creators and be available at DistroWatch. No site visits were necessary. The class had more than 60 students including a mix of graduate and undergraduate students. The graduate students on each project served as the project managers. The project will continue through the summer.

This concept need not apply only to academic classes. On several occasions the course work was augmented by assistance from the computer club, (which I advised) which facilitated assessing donated computers, wiping hard drives, installing Linux and OpenOffice. One project with the local Rotary club had students create a resource center in Belize (yes, the projects have had international impact, too!).

I do require nondisclosure agreements and releases of liability on all sides (students and nonprofit organization). All participants receive letters on letterhead from the assisted organization thanking the student by name for their contribution (for security and privacy, the address used is that of the school). The appropriate level of jargon and specifics is included as I

write the letters and I remain the point of contact for confirmation of their efforts and experience so the nonprofit is not overwhelmed with calls for references. All students can list their participation on their resumes as volunteerism and work experience.

As proof of concept I offer the award I received in June 2017 at the Community College Cyber Summit (3CS) for Teaching Innovation in the area of Community Outreach (won under my former name: Denise Pheils) and the research behind this community project method which was presented at the 2013 ACM InfoSec Curriculum Development Conference at Kennesaw State University and was published as:

Pheils, D. (2013). Applying a Community Project Approach to IT and Security Courses. In *Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference* (InfoSecCD '13). ACM, New York, NY, USA, , Pages 79 , 9 pages. DOI=http://dx.doi.org/10.1145/2528908.2528924

Cybersecurity Law for Undergraduates

By Jeff Kosseff[1]

Abstract: Undergraduate cybersecurity programs can – and should – educate students about cybersecurity law. This Paper outlines the U.S. Naval Academy's approach to the cybersecurity law class that is required for undergraduate cyber operations majors. Although the students have no previous legal education, they grasp many of the complex laws relevant to cybersecurity professionals. A successful undergraduate cybersecurity law class provides a foundational overview of legal concepts, integrates current events, evaluates students' written and oral communication skills, and requires students to think critically about legal issues.

In 2016, the United States Naval Academy graduated its first class of cyber operations majors – 27 midshipmen out of about 1,100 graduates. Two years later, the ABET-accredited program has quadrupled in size, with 110 freshmen choosing the major.

The Naval Academy requires all cyber operations majors to complete a cybersecurity law class, usually in their final semester. I joined the Naval Academy faculty in fall 2015, and I spent much of that semester designing the new class. I spoke to cybersecurity lawyers and operational professionals in the military, civilian government, private sector, and civil liberties groups. Most of the experts agreed on a core set of topics that they would like to see in an undergraduate cybersecurity law class.

I filled a whiteboard with more than 100 possible topics, but I did not yet have a structure for the class. I faced two primary challenges. First, I needed to whittle down the list to a manageable set of topics for a semester-long course. Second, the Naval Academy is an undergraduate institution. Law school students typically can take cybersecurity law as an elective in their second or third years, after completing the required first-year classes on contracts, criminal law, torts, property, and civil procedure. Undergraduate students, in contrast, have not received that foundational legal education before enrolling in cybersecurity law.

[1] Assistant Professor, Cyber Science Department, United States Naval Academy. The views in this article are only those of the author, and do not represent the U.S. Naval Academy, Department of Navy, or Department of Defense.

I attempted to structure the class in a logical format that tells the story of what we generally conceive of as cybersecurity law, moving from broad constitutional contours to more specific laws, and concluding with international cybersecurity norms. The class is broken into five general units, each consisting of approximately three weeks of classes:

- **Constitutional Foundations of Cybersecurity Law:** Executive power; legislative power; judicial review, and constitutional liberties (First, Fourth, Fifth, Tenth, and Fourteenth Amendments).
- **Statutory Foundations of Cybersecurity Law:** Statutory authorities for government cyber operations (with a focus on Titles 6, 10, 18, 32, and 50 of the United States Code); statutory limits on government cyber operations and surveillance (Electronic Communications Privacy Act and Posse Comitatus Act); foreign intelligence surveillance (FISA, Executive Order 12333, and PATRIOT Act); and division of governmental responsibilities for U.S. cybersecurity among federal and state agencies.
- **Private Sector Cybersecurity Law:** Federal Trade Commission data security actions; sectoral data security laws; state data security and breach notification laws; data breach litigation; attorney-client privilege for cyber forensics investigations; cyber-threat information sharing; encryption and the All Writs Act; privacy law; and General Data Protection Regulation.
- **Computer Crime and Hacking Laws:** Computer Fraud and Abuse Act; state computer crime laws; Section 1201 of the Digital Millennium Copyright Act; and Economic Espionage Act.
- **International Cybersecurity Law:** Law of war in cyberspace (jus ad bellum, jus in bello, cyber sovereignty, and jurisdiction); Budapest Convention.

Because Naval Academy students have not received a first-year law school education, each section begins with a general overview of the foundational concepts that underlie the legal issues. For instance, the Constitutional Law section begins with a brief history of judicial power dating back to *Marbury v. Madison*, and the Private Sector Cybersecurity Law section includes an overview of the stages of civil litigation.

Law school classes typically evaluate student performance almost entirely based on final-exam performance. The final exam usually requires a student to identify and analyze issues in lengthy

hypothetical fact patterns. This allows the professor to evaluate a student's ability to spot legal issues, identify applicable legal rules, and analyze how those rules apply to the facts in the hypothetical. The law-school grading model does not work well for the Naval Academy, which requires grades at the six-week, 12-week, and final exam period. Nor does the model adequately evaluate other skills that we hope to teach our cyber operations majors, including presentation delivery and expository writing. Accordingly, each student is evaluated based on the following assignments:

- A hypothetical issue spotter mid-term exam
- A term paper on a current cybersecurity law issue of the student's choice, and a class presentation about the topic
- An in-class appellate argument in which students argue for and against the reversal of a district court cybersecurity-related opinion, with practicing lawyers and faculty as judges
- A final exam with 2-3 hypothetical issue spotter fact patterns
- Two in-class presentations about current events in cybersecurity law
- Class participation

I have taught nine sections of the class since Spring 2016, and have honed the material each semester to ensure it is current. Based on this experience, I conclude with the following lessons:

- Undergraduates are far more capable of learning complex cybersecurity law concepts than I had expected. This is partly because most of the students are seniors who have taken a number of challenging technical cybersecurity classes; thus, they can understand some material more easily than technological novices. For instance, when I teach the encryption dispute between Apple and the FBI, the students already are familiar with the mechanics of encryption, allowing us to focus on legal concepts such as the All Writs Act.
- Cybersecurity law is rapidly evolving, requiring constant evaluation of course topics for currency. For instance, after courts issued many Fifth Amendment opinions regarding compelled unlocking of smartphones, I added a section about the topic. Many legal issues, such as the Fourth Amendment and the Computer Fraud and Abuse Act, always will be relevant to cybersecurity law. Current event presentations help to ensure that students critically analyze new developments in cybersecurity law.

- Undergraduate cybersecurity law classes should not aim to prepare students to perform the work of lawyers; indeed, unless the graduate has a juris doctor and active bar admission, such work would be illegal. Instead, the undergraduate cybersecurity law class should expose students to the fundamental legal issues that they will encounter throughout their careers in cybersecurity, and to understand when they need legal advice. The class also should cause students to think broadly and critically about the role of the cybersecurity profession in a society of laws and norms.
- Cybersecurity education is not a binary choice between technical and non-technical subjects. The students in my class apply their technical knowledge to the relevant laws, resulting in productive discussions. For instance, when we assessed the privacy implications of the Dark Web, much of the class involved a discussion of the mechanics of TOR. Relatedly, students tell me that the cybersecurity law class causes them to think carefully about the legal implications of their technical cybersecurity research.
- The course is most effective when it forces undergraduates to critically evaluate not only how current laws shape cybersecurity, but also how future laws *should* affect the field. As future cybersecurity leaders in the private sector or government, they may have the ability to shape the rapidly evolving body of cybersecurity law.

NACE Workshop Position Statement – Cybersecurity Education and Competency Challenges

Nancy R. Mead, PhD, SEI Fellow Emeritus, CMU Adjunct Professor of Software Engineering, nrmcmu@gmail.com

Bio Sketch: Dr. Nancy R. Mead is a Fellow Emeritus of the Software Engineering Institute (SEI), and an Adjunct Professor of Software Engineering at Carnegie Mellon University. Her research areas are security requirements engineering and software assurance curricula. The Nancy Mead Award for Excellence in Software Engineering Education is named for her.

Prior to joining the SEI, Mead was a senior technical staff member at IBM Federal Systems, where she spent most of her career in the development and management of large real-time systems. She also worked in IBM's software engineering technology area and managed IBM Federal Systems' software engineering education department. She has developed and taught numerous courses on software engineering topics, both at universities and in professional education courses.

Mead has more than 150 publications and invited presentations. She is a Life Fellow of the IEEE, a Distinguished Member of the ACM, and was named the 2015 Distinguished Educator by IEEE TCSE. Dr. Mead received her PhD in mathematics from the Polytechnic Institute of New York.

Position Statement: Let us consider challenges in cybersecurity education and its associated competencies:

- Cybersecurity these days must consider much more than shoring up an existing system's defenses and applying patches.

  Although cybersecurity was once limited to such concepts as patch management, firewalls, and encryption, it has become clear that such methods are far from adequate for today's threats. Unfortunately, many managers are still stuck in a time warp that leads them to think that cybersecurity is something that only needs to be considered after a system is fielded. As a consequence, systems are developed that can never be adequately secured due to poor architecture and implementation decisions. There is a substantial need to educate people who are still laboring under these misconceptions.

  These same folks do not know what to do with graduates of modern cybersecurity programs, and relegate them to low-level positions in system administration just to fill a slot (I call this "cannon fodder"). The highly qualified individuals hired into these slots can't wait to "do their time" and find a more interesting job, and some of them even buy their way out of a contractual obligation in order to do so.

- When they hire, employers tend to look for experience in specific languages and tools, rather than more substantial competencies. Moreover, career advancement in cybersecurity seldom includes defined competencies as a consideration.

  It's probably been at least 5 years since I pointed out that classified ads do not seek individuals with substantial educational background. Instead, they advertise for expertise in specific languages, specific static analysis tools, and so on. Moreover, they don't want to train new employees, but expect them to be productive out of the box. This occurs in part because people change jobs often, and employers don't want to invest in growing the skills of people who will be gone in a year.

  On the plus side, there are some organizations who have developed competency models for cybersecurity and software assurance. How they are being used, however, is largely unknown.

- At all levels of education, there is a dearth of faculty who are qualified to teach cybersecurity.

  In attempting to transition software assurance curriculum recommendations, especially at the community college and high school levels, it is clear that there are not enough qualified faculty to do this. If the school has degree offerings in computer science or information systems, then the existing faculty can learn enough about the field to be able to teach it. However, faculty members who are

set in their ways are not necessarily motivated to change. One possible solution is to bring in adjunct faculty to teach these courses, but quite frankly, for someone in industry, adjunct salaries usually amount to what I call “charity work”. If you consider all the hours put in, the salary doesn’t even amount to minimum wage.

On the plus side, whenever software security and software assurance degrees are offered, there seem to be an ample number of students who are interested in these offerings. In undergraduate and graduate programs, more cybersecurity degree offerings exist than at the lower levels, but there is a risk that students will rush into these programs because the field is “hot”, and later as graduates, lose interest and drop out of the field, much as we saw in computer science some years ago.

- For the most part, standard sets of material for teaching a cybersecurity or software assurance curriculum at any level are not publicly available.

  Although some faculty are willing to make their material publicly available, it is often the case that the material is considered the intellectual property of the university or the individual faculty member. Individual faculty members who use the same material to do consulting or teach industry workshops are reluctant to share their materials with others who may have similar consulting arrangements. Universities may be reluctant to have material shared if they think it helps a competitor. With online and distance education offerings, any university can be considered a competitor, regardless of their physical location.

  Government-funded projects have helped to address this, but the funding is usually insufficient to support fielding an entire program, and it can’t be counted on from one year to the next. If it is done, it is usually a one-time effort, with no opportunity to refresh and modify the material at a later time. The funding, when it exists, is often used to support making course materials available “as is”, without consideration of how to make it useful to other instructors who are not teaching the exact same course at the same university. By and large, there is no data collected on how many faculty use publicly-provided material, or how effective it was, assuming measures of effectiveness even exist. Needless to say, the same applies to students who are on the receiving end. Sad to say, it’s possible to get a grant to support a single workshop, or what is otherwise a volunteer effort, but grants to support a substantial amount of work are seldom available.

- Possible solutions

  Given the challenges, it may appear that this is a nearly impossible problem to solve. However, I believe that a cooperative, appropriately funded, multi-year effort between government, industry, and academe could go a long way.

  The NICE framework attempts to address some of the issues, but it seems to be largely concerned with managing the effort, rather than developing content, and once again depends on voluntary participation and donated materials. Possibly it could serve as more than just a clearing house for materials, although it too appears to involve a revolving door of managers who are there for a year or two, and probably the funding varies from one year to the next as well. The Scholarship for Service program certainly produced a number of graduates with excellent background, although it's not clear whether it could/should continue. Ditto for the Centers of Academic Excellence. Certainly government needs to be a long-term part of the solution.

  Industry needs to recognize that this is not simply a case of telling educational institutions what skills are needed from graduates, so that they can be productive from day one. Higher education is intended to produce individuals who have learned the fundamentals that will serve them well over the course of their careers – the ability to create, learn, apply, and analyze problems, approaches, and methods that may not even exist when they graduate.

  Considering the fact that information systems and cybersecurity now concern all of us in our daily lives, educational institutions at all levels need to collaborate to support the development and delivery of appropriate course materials. This is not a time for stove-piping.

  Measures of effectiveness need to be defined and built into educational program follow-up. It is not sufficient to do something once and then declare victory. It takes resources to track graduates over a period of years, collect feedback, and use the feedback to improve present and future programs.

  All of this takes dedication, and resources. It's not something that can be tossed off in a year or two. While it is certainly the case that progress has been made, more is needed.

  [Generic reference due to word count limit! https://www.sei.cmu.edu/education-outreach/curricula/index.cfm]

Interdisciplinary Cyber Security Education

Randal Milch and Nasir Memon

New York University

NIST's National Initiative for Cybersecurity Education (NICE) is a crucial step toward remedying the Nation's undeniable shortage of "people with the knowledge, skills, and abilities to perform the tasks required for cybersecurity work." Such a workforce will include "technical and nontechnical roles that are staffed with knowledgeable and experienced people."

The NICE Cybersecurity Workforce Framework goes on to identify 7 workforce categories, which encompass 33 specialty areas and over 50 work roles. A review of the specialty areas and work roles shows that – in many crucial areas – an "integrated cybersecurity workforce" is not split between "technical and non-technical roles." Within the seemingly non-technical "Oversee and Govern" workforce category for instance, every work role in the Legal Advice and Advocacy, Strategic Planning and Policy and Executive Cyber Leadership Specialty Areas requires technical knowledge of "computer networking concepts and protocols, and network security methodologies." (K001). Similarly, every work role in the apparently technical "Securely Provision" workforce category, requires quintessentially non-technical knowledge of "laws, regulations, policies, and ethics as they relate to cybersecurity and privacy." (K003).

The question, then, is how to produce a workforce with these inter-disciplinary skills. Recent and laudable strides made to create more cybersecurity engineers at do not require a law and policy course for masters candidates on the technical track.[1] Similarly, Professor Chesney's recently published and excellent syllabus for his "Cybersecurity Foundations: Law, Policy, and Institutions" course has no technical component for law and policy students without technical training.[2]

We propose that a critical component to an interdisciplinary need is actual

interdisciplinary instruction. For two years, the authors have taught a seminar in which JD and LLM students at NYU Law School and MS and PhD students at NYU Tandon School are instructed together. The class's premise is that technology and policy are interdependent in cyberspace.

We posit that the key to intelligent application of the disparate regulatory and policy schemes with which we confront cyberinsecurity – and the basis for intelligent development of law and policy – is a thorough understanding of the technology that underlies the current and future security of the Internet. At the same time, the engineers who build products and solve problems can increase the range of policy choices if they appreciate the range of policy needs and legal/compliance requirements, including those that are inefficient or counter-intuitive from an engineering point of view.

Our seminar aims to bring the relevant technology and the current legal landscape together, for a richer understanding of each. The seminar seeks to impart the following key cybersecurity engineering concepts:

- Understand threat, vulnerability and risk;
- Basic concepts of security - confidentiality, integrity and availability, and the means for achieving these properties in a system;
- Basic concepts related to how the Internet works - packet switching, routing, DNS, etc.;
- Understand how anonymity can be provided while communicating on the Internet and why attribution of attacks is difficult;
- Problems related to identity and authentication.

And the following key cybersecurity law and policy concepts are taught:

- How rules are made with respect to cybersecurity and who makes the rules – legislators, regulators and private groups;
- The roles and responsibilities of the government and private parties in

protecting networks;

- What companies are obligated to do with respect to cybersecurity;
- Issues surrounding voluntary information-sharing (public/private and private/private);
- How regulation and private civil litigation are defining "reasonable" cybersecurity measures;
- Obligations to provide information to and cooperate with government (intelligence, law enforcement, data vs. metadata):
- Data privacy regulation (EU vs. US) and its impact on cybersecurity (e.g. insider threat monitoring).

Students are placed in interdisciplinary groups to tackle problems from both technical and legal/policy angles. Responses to the course have been favorable, and it is clear that both the engineering and the law students take away a new and valuable literacy with one another's chosen fields. It is also apparent that the difficulties in cross-training are not equal. It is easier to provide engineering students with instruction in law and policy than it is to provide law students will little or no technical background with meaningful technical instruction.[3]

Efforts at the graduate level, however, ignore the large cybersecurity workforce already in place. Steps must be taken to provide existing cybersecurity professionals without interdisciplinary training with a route to obtain the knowledge they need to excel in their role. Based on the success of the graduate-level seminar, NYU is seeking to meet this need through a new Executive MS in Cybersecurity Risk and Strategy offered jointly by NYU School of Law and NYU Tandon School of Engineering.[4] The one-year program is intended for experienced professionals from a range of backgrounds who seek to deepen their understanding of cybersecurity risk and strategy. This program will create managers with the integrated expertise needed to play a leadership role in the field.

The MS in Cybersecurity Risk and Strategy program is a 30-credit executive MS management degree incorporating both online courses and blended-learning modules. Over a 12-month period, participants attend three residential sessions consisting of five days per session. Between residential periods, students are expected to study 10-15 hours per week in online and blended-learning formats. Semesters are divided into three phases: online introduction, in-class residency, and online implementation.

In order to ensure a common foundation for students from widely disparate backgrounds, MS-CRS students must, before starting their credit-bearing courses, pass on-line "bridge" courses in U.S. Law and in the technical Foundations of Cybersecurity. Each semester includes a 3 credit, core engineering course (Information Security and Privacy, Network Security, and Information Systems Security Engineering and Management) and two law or policy courses (such as Information Privacy Law, Cybersecurity Governance and Regulation, Cyber Crime and Innovation Policy) bearing a total of 5 credits. Spanning all three semesters is a 6 credit, team-based "Integrative Cybersecurity Management" Capstone Project.

Author Bios

Randal Milch is the Co-Chair of the NYU Center for Cybersecurity, a Distinguished Fellow at the Center on Law and Security, and a Professor of Practice at NYU School of Law

Nasir Memon Nasir Memon is a professor in the Department of Computer Science and Engineering at NYU Tandon. His research interests include digital forensics, biometrics, data compression, network security and security and human behavior.

[1] On-line students in the Georgia Tech program who chose a "Policy specialization" would be hard-pressed to avoid at least one law or policy course.

[2] Importantly, Professor Chesney hopes to attract "grad students . . . in business, engineering, and computer science" to his course.

[3] Law students *with* a technical background, however, are perhaps the most adept at mastering the combined material.

[4] The authors serve as Faculty Co-Directors of this new Program.

THE REVIVAL OF THE APPRENTICESHIP: A NEW APPROACH TO CYBERSECURITY EDUCATION (NACE) WORKSHOP CONCEPT PAPER

by

Lauren Neely, JD

The job titles in cyber security vary, as do the skills, experience, and tools needed to successfully perform the duties demanded by those titles. The skill set that might prepare a potential employee to be a Security Analyst will not be the same skill set needed to work as a Security Software Developer or Engineer or a Security Consultant. For instance, a security software developer may require a greater knowledge of programming languages, web development, agile methodologies, and cloud computing. For this reason, I propose that the best way to address the levels of education and training needed for future cyber security professionals and the cyber security labor supply issue is through the revitalization of the apprenticeship model of workforce development. Programs such as the National Science Foundation's Scholarship for Service program have made important contributions for students who will work for federal agencies upon completing their education, but a similar effort needs to be embraced by industry. Apprenticeship programs are unique in that they often align education with on-the-job training and have the added benefit of ameliorating a persistent problem facing entry-level or career transistioners looking to move into the industry. In order to get a job they need experience, but they cannot get experience because employers can ill afford to take a chance on untried entry-level employees. Sources have recognized the current disconnect between the claims of thousands of unfilled cyber security positions and the new graduates and potential employees who have tried to break into the field unsuccessfully because they lack the requisite experience.[1] Apprenticeship programs can fill this gap.

According to the U.S. Department of Commerce,

"Apprentice programs work – not only because they help employers find exactly the trained talent they need but because they help people quickly enter a field, without college debt or an exhausting job search. Apprentices tend to be loyal workers because their employers have invested in them both on the job and through educational assistance to help advance their careers. This has shown to reduce employee turnover rates and increase morale."[2]

The National Initiative for Cybersecurity Education (NICE) led by National Institute of Standards and Technology (NIST) and at US Department of Labor's Office of

[1]Tripwire, The State of Security: News, Trends, Insights. "Talent Shortage Sanity Check." https://www.tripwire.com/state-of-security/risk-based-security-for-executives/connecting-security-to-the-business/talent-shortage-sanity-check/ retrieved April 30, 2018.
[2]U.S. Department of Commerce, Apprenticeship Works for the IT Industry, https://www.commerce.gov/news/blog/2018/01/cybersecurity-apprenticeships-enhance-cybersecurity-infrastructure retrieved April 30, 2018.

Apprenticeship offers support and guidance for those looking to build an apprenticeship program, but to date only a handful of these programs are in operation. It is incumbent upon local employers, educational institutions, and cyber security professional organizations to work together to create viable apprenticeship programs. These programs will serve to alleviate the labor shortage and allow for a more diverse cyber security workforce by actively recruiting women and minorities as apprentices.

Lauren Neely received her J.D. from the University of Houston Law Center. Upon graduating from law school, Lauren worked for a commercial real estate advisory firm for several years before deciding to return to the public sector and her alma mater, the University of Houston. Lauren served in several capacities during her return stint to the University of Houston and is the former Assistant Director of the Hobby School of Public Affairs. In 2017, Lauren joined the University of Houston Law School Street Law Program as a co-instructor. Lauren is a member of the State Bar of Texas and is currently pursuing a Master's in Cyber Security Operations and Leadership at the University of San Diego.

Futuristic Cybersecurity Education and Workforce Development Initiatives

A Proposal by Amos Olagunju, IT Professor

St Cloud State University, St Cloud, MN

0. Foreword

The survival of the current and future cybersecurity workforce will depend on effective strategies for the recruitment, retention, and continuous educational training of diverse students in high schools, two and four-year academic institutions. This proposal provides justifications and advocates initiatives for continuous successful recruitment, retention and training of diverse students for sustaining cybersecurity workforce.

1. Recruitment

Four-year academic institutions should form partnerships with local or nearby high schools and technical and community colleges, to sustain the recruitment of diverse students for associate or bachelor's degrees in areas relevant to cybersecurity. Today many academic institutions promote and support experiential training for students in the areas of computer science, information technology, and cybersecurity. Essentially, current computer science, cybersecurity and information technology degree programs that mandate experiential learning or capstone requirements should engage and mobilize more students to serve as role models for recruiting students from high schools and two-year institutions. College students should be guided by faculty and staff members to design academic and co-curricular skill-enrichment mathematics and computing activities for motivating youngsters to pursue bachelor's degree programs in cybersecurity and related areas. The enrichment activities should be delivered by college students to high schools on convenient periodical schedules.

Faculty members at four-year academic institutions ought to sign more articulation student transfer agreements with two-year institutions that offer associate degrees in areas related to cybersecurity education. Moreover, faculty members at two and four years institutions in areas of cybersecurity should meet periodically, to review and recommend changes in the educational training of students at two-year institutions for successful careers.

2. **Retention**

Clearly, it is not enough to recruit diverse students into cybersecurity programs without a strategic plan to cope with students who end up struggling with core courses in areas such as mathematics and computer programming. A comprehensive cybersecurity program in associate or bachelor's degree ought to have alternative plans for guiding students with deficiencies in mathematics, scripting, programming, and/or installation and applications of cybersecurity tools to success. Retention strategies might include the use of currently high-achieving cybersecurity majors or alumni or industrial partners to mentor and serve as role models to future cybersecurity experts. Retention of minority students in cybersecurity programs might be considered intrusive, but there is reason to believe that a carefully outlined alternative plans for guiding students with various academic, family, social and financial issues, will promote more diverse students for the cybersecurity workforce.

3. Cybersecurity Skill Training Requirements

The question naturally arises on the skills required for graduates with two-year or four-year degrees in cybersecurity. Should associate and bachelor's degree programs in cybersecurity be designed and offered based on the existing and future anticipated faculty strength? Regardless of the faculty strength what skills should graduates with associate or bachelor's degrees in cybersecurity demonstrate upon graduation, and perhaps in long-life learning?

In agreement with the ABET requirements for the accreditation of current and future cybersecurity programs, herein are long-life skills for future cybersecurity training:

Student learning outcomes for cybersecurity majors should mirror the ability to:

1. Write correct, well-documented and readable programs.
2. Describe and use networks.
3. Describe and use operating systems.
4. Articulate ethical, professional, and legal standards of behavior.
5. Communicate effectively in written and oral exchanges.
6. Design and implement secure network architecture based on security policies.
7. Identify and correct security weaknesses in operating systems, networks, and applications.
8. Demonstrate understanding of theoretical foundations of security by solving problems.

9. Design and implement effective defensive and offensive strategies in cyber security.

But, what kinds of courses should be designed to satisfy the current and future needs of cybersecurity workforce? Here are a few examples:

- A Course in Firewall and Penetration Testing might include Knowledge of common network tools:
    - Knowledge of Computer Network Defense and vulnerability assessment tools, including open source tools, and their capabilities
    - Knowledge of Defense-In-Depth principles and network security architecture
    - Knowledge of general attack stages Knowledge of network security architecture concepts including topology, protocols, components, and principles
    - Knowledge of penetration testing principles, tools, and techniques
    - Skill in applying host/network access controls
- A Course in Offensive and Defensive Security might cover:
    - Knowledge of different classes of attacks
    - Knowledge of front-end collection systems, including network traffic collection, filtering, and selection
    - Knowledge of host/network access controls
    - Knowledge of incident response and handling methodologies
    - Knowledge of intrusion detection system tools and applications
    - Knowledge of network traffic analysis methods
    - Knowledge of the common attack vectors on the network layer
- Applied Cryptography
    - Knowledge of cryptology
    - Knowledge of encryption methodologies
    - Knowledge of network access, identity and access management
- Database
    - Knowledge of database management systems, query languages, table relationships, and views
    - Knowledge of database theory
    - Knowledge of query languages such as SQL

    - Skill in developing data models
    - Skill in generating queries and reports
    - Skill in maintaining databases
    - Skill in optimizing database performance
- Operational Safeguards
- Knowledge of policy-based and risk adaptive access controls
- Knowledge of current and emerging threats/threat vectors
- Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins
- Knowledge of system and application security threats and vulnerabilities
- OSI Layer Security
- Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol (TCP) and Internet Protocol (IP), Open System Interconnection Model (OSI), Information Technology Infrastructure Library, v3 (ITIL))
- Knowledge of IA principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation)
- Knowledge of network security architecture concepts including topology, protocols, components, and principles
- Knowledge of VPN security
- Skill in securing network communications
- Computer Forensics
- Knowledge of anti-forensics tactics, techniques, and procedures
- Knowledge of basic concepts and practices of processing digital forensic data
- Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data
- Knowledge of seizing and preserving digital evidence
- **Security Policy and IT Risk Management**
- Knowledge of Computer Network Defense policies, procedures, and regulations
- Computer Networks
    - Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services

Summary

The industry is already infusing DevOps tools and agility into business operations. The need exists to develop case-based projects for training the future cybersecurity workforce about agile skills and rapid applications and network monitoring using DevOps tools. If I have the opportunity to participate in this panel discussion of the long-overdue recruitment and retention of the Cybersecurity Workforce, I will be willing to demonstrate creative projects that can be used to motivate, recruit, and retain more students into the current and future cybersecurity workforce.

Bio Sketch of Amos Olagunju

Amos Olagunju is a professor in the Computer Science and Information Technology Department at St. Cloud State University (SCSU) in Minnesota. He previously served as the interim dean of undergraduate studies at SCSU. Under his leadership, SCSU experienced the highest levels of enrollment, retention and graduation of students for minority students in STEM areas. He has served as the School of Graduate Studies Dean and Chief Research Officer at Winston Salem State University. A faculty fellow and later a senior faculty fellow selected jointly by the American Society of Engineering Education and the Navy, Amos developed manpower mobilization and data-mining algorithms for monitoring the retention behaviors of personnel. Under the leadership of Amos as a Professor and Chair of the Computer Science Department, Delaware State University established a reputable computer science degree program for minority students. As a visiting scholar at Michigan State University, he investigated the barriers to the retention and graduation of minority students in computer science and published a solution manifesto for international audience in computer science education. Amos is an ABET Program Evaluator. He has participated in the Carnegie African Diaspora Fellowship Program and the Specialist Fulbright Scholar Program.

Dr. Stephen R. Orr IV is currently the National Security Agency (NSA) visiting Professor for Cyber Security Studies at the United States Naval Academy. He holds a Ph.D., M.S., and B.S. degree in Computational and Information Sciences. Dr. Orr has held analytical, technical, operational, and leadership positions at both Headquarters and the field. His expertise and career has focused on offensive and defensive cyberspace operations. Most recently, Dr. Orr was part of a team that won NSA's prestigious Deckert/Foster Award for Excellence in SIGINT engineering.

Dr. Orr's most recent assignment was the Executive Director of J3, Operations for United States Cyber Command. In this capacity he was responsible for directing command operations spanning from future planning, through operations execution within the authorized computer network operations mission space.

Dr. Orr's research interests include the intersection of cybersecurity and human factors, cyber effects, and the application of emerging technologies.

This proposal attempts to address the challenge of what a follow on Scholarship for Service (SFS) could look like in the twenty years since it was first established, while addressing multiple general topic areas to cybersecurity education. It is through this proposed academic construct that private and public sector challenges could be addressed. Simply put, it is proposed that we evolve the **centers of academic excellence construct to focus on the "*at least three dozen specializations*" that exist in the cybersecurity discipline**. Diversifying the expertise at any one academic center of excellence has the ability to produce many students that are average at everything, and good at nothing. By restructuring the fundamental institutional model, these centers of academic excellence **and specialization** would create a monopoly on **producing expertise** in one of the many subdisciplines of cybersecurity. In turn, students would graduate with the broad liberal arts education that inspires creativity and critical thinking, complemented with specialized skills to meet the private and public sector cybersecurity challenges. Furthermore, this institutional construct provides a gateway for solving the more general topic areas of cybersecurity education.

The National Security Agency (NSA) originally created the Center for Academic Excellence in Information Assurance Education (CAE-IAE) in 1998, with the Department of Homeland Security (DHS) joining as a partner in 2004. Since that time te CAE in IA Research component was added in 2008 to encourage universities and students to pursue higher-level doctoral research in cybersecurity. Later, the CAE-Cyber Operations program was established, which focuses on technologies and techniques related to collection, exploitation, and response. This construct has, and continues to pay dividends to enhance the national security posture of our Nation. **The specialization designator allows academia to take the lead by voluntarily constructing a monopoly on specialized cybersecurity education**. This evolution would further enhance the NSA and DHS sponsored Centers of Academic Excellence, while also "future-proofing" the education we provide.

To be clear, it is not proposed that these institutions would **only teach** any one of the subdisciplines of cybersecurity. Nor that there would be only once academic institution to focus on any one specialization. **Specialization requires a solid foundation and core competencies**. For example, a fundamental understanding of computational and information concepts such as programming, operating systems, and networking; policy, legal, and ethics would be necessary. Each of the documented specializations would further focus on these

particular areas allowing the academic center of excellence to be designated as producing graduates with a particular specialty. However, given this is a dynamic field it is guaranteed that the specialization requirements of tomorrow will not be the same as the specialization requirements of today. This proposal allows for academic institutions to adapt to meet the specialized requirements without significantly disrupting their entire academic program, as the fundamental core competencies will remain the same. Collectively, academia would meet the demands of private and public institutions today, while having the ability to adapt and change to the dynamic needs of the future. **Thus, "future-proofing" the academic education through specialization is achieved by adapting to the cybersecurity challenges of today and tomorrow, while providing a core foundation in computation and information science concepts**.

The proposed academic centers of excellence and specialization **creates a natural opportunity to partner with cybersecurity vendor-neutral training and certification providers, or supplanting them by meeting the needs of the market they currently fill**. Vendor-neutral certifications typically validate a candidate's unbiased knowledge or skills of a particular technology principles. This is done through traditional tests and hands-on, skill-based scenarios. The specialization designator lends itself to providing more specific, short-term knowledge and skills to meet the demands of today. This specialization, combined with a traditional broad understanding of computational and information sciences provides a win-win-win scenario for the student, academia, and industry. An academic institution that currently offers a version of this proposal is the University of Maryland University College (UMUC). They offer technical programs that combine broad understanding of fundamental computation sciences with cybersecurity training and certification to meet industry demands. Creating academic centers of excellence and **specialization** could build and improve upon this model while increasing value of a college education. **Specialization through academic centers of excellence creates centers of gravity to address the mix of education methods, industry practice, and government needs**.

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.

Onramp to cybersecurity Labor Pipeline through K12 Classroom Education

Meg J Ray
Teacher in Residence
Cornell Tech

Tim Winston
Principal, PA-QSA(P2PE), CTGA, CISSP, CISA
Coalfire Systems

Key to solving labor supply issues in cybersecurity is a strategy that begins well before college. To achieve a diverse pipeline of cybersecurity professionals and a populace educated in basic data privacy and security concepts, we must build and fund a coherent K12 strategy that makes sense in our current school system and brings together the expertise of cybersecurity and education specialists.

The primary need is a future-proof and readily available labor pipeline in the US. The impact of Moore's Law on all current technology spaces (ie. mobile devices, cloud computing, IOT) not only applies to increasing computational power but more generally to the exponential expansion of all types of capabilities. Given this circumstance, future proofing our workforce will not be about anticipating technological development, but about preparing professionals who can assimilate new technologies quickly, apply foundational concepts in novel situations, and are fluent in metacognitive skills. Although students will still require areas of technical proficiency, this mindset requires a shift in our approach to education. Students will still need to develop one or two areas of technical proficiency. This will allow incoming professionals to fully appreciate how to secure and apply cybersecurity principles, to one area that they understand deeply before generalizing to a wide range of technologies.

Technical roles are not the only need to be addressed in cybersecurity labor supply. The technically oriented attacker and defender roles may be the first and only ones that come to mind, but there are many others on a team that are vital to supporting these roles. In the cybersecurity field we also need skilled project managers, educators, designers, and grant managers. People who do not have the interest or opportunity to pursue the engineering side, need to know that there are still critical careers in cyber security where they can make a crucial contribution.

A secondary need that K12 education can address is a cybersecurity literate population. This type of general literacy can only help the efforts of cybersecurity specialists on a broad scale. A better understanding of security and privacy is more important than ever: policy makers at all levels, developers and data scientists, CEOs and CFOs in all industries, and voters. It is of vital importance that individuals across industries understand the value of, and threat to, their personal and professional data. In this way individuals would better understand and support the need to properly protect information.

We can lift important lessons from recent efforts to broaden access and awareness in STEM and CS education. Early positive math and science experiences and career awareness, especially at the middle school level, is important to recruiting interest particularly for underrepresented student populations (Maltese & Tai, 2011; Moakler & Kim, 2014). Leaving relevant classes and experiences only to those who opt in, excludes large numbers of talented students. Barriers include issues of student identity and obstacles to access, such as needing to hold an after school job or attending a school that does not offer AP classes (Margolis, 2008; Wang & Degol, 2013). To address these needs, we propose a multi-pronged approach touching all levels of K12 education.

First, all children need a basic understanding of how the digital world works. As outlined in the K12 CS Framework, they should understand the basics of computers, networks, and data. In order to recruit interest in cybersecurity and prepare students for required classes, it is important that they do not leave high school with the vague idea that it works "somehow" or by "magic." Children's innate temptation to misuse things can actually be a positive indicator for both STEM and specifically security. Rather than simply correct the impulse - it can identify the aptitude and redirected to the importance of building and testing securely. These concepts can be fit into CS, technology, or science classes. Elementary school students are introduced to these concepts through the use of stories and physical activities that model computing processes. As students move up, they are able to learn lower level concepts and incorporate them into projects that reflect real world contexts.

In middle school, many schools begin to teach digital citizenship. There is a tendency in CS education to draw a hard line between technology/digital citizenship and computer

science/coding. We need to soften this line and reboot our middle school curriculum. Digital citizenship education 2.0 must involve more than anti-cyberbullying campaigns. Students should learn web safety as well as web development. They learn to not give their personal data to strangers, but should also learn how their data is tracked with routine web use and how to secure and protect their own data.

In high school, it is appropriate for all students to learn and think about the current and historical context of cybersecurity. In social studies classes, units should be supplemented to include themes related to surveillance, privacy, protecting our capabilities, ethics, etc. They should understand personal and national security as themes in wartime and peacetime and how historical events have impacted current issues.

In high school, we can broaden current CS learning for students who are taking higher level math and CS courses to prepare for STEM careers. CS classes need to incorporate opportunities for students to have counter functional experiences, by “breaking” each other's work and by finding new use cases. This “make it, then break it” approach also addresses practices and metacognitive skills in the K12 CS Framework that are more difficult to teach. For example, we want students to understand that projects are never just done. There are always iterations that can be made based on need and context. We also want students to know that making something work technically is just as important as developing soft skills like problem solving, self-reflection, and project management. We can open the doors of CS experiences such as robotics clubs and engineering classes to a wider group of students by explicitly creating and valuing roles project manager or publicist.

In order to make this K12 strategy a reality, two areas need to be addressed. First, we need quality curriculum disseminated effectively to teachers. This type of curriculum is best developed within partnerships between education and cybersecurity experts. Disseminating curriculum means building partnerships with trusted education websites across disciplines. Teachers cannot teach curriculum that they do not know about. Second, we need to train teachers. Unfortunately, cybersecurity is an area about which many lay people hold misconceptions. Looking again to recent developments in CS education, we know that professional development is a complex problem to address due to issues of scale, fidelity, and

teacher interest and capacity (Pollock, et al., 2017). However, a blend of online and in-person training as well as partnerships with school districts, non-profits, industry, and universities, makes it possible. The approach we have outlined is built for minimal change in the school day and is a relatively light lift, based on doable changes such as supplementing lessons or units in existing curriculum. If stakeholders in K12 education, universities, and industry work together, it is possible to create an effective primary and secondary education strategy that will be the cornerstone of cybersecurity literacy in the general population and play a key role in increasing and diversifying the cybersecurity labor pipeline in our country.

BIO SKETCH

Tim Winston | PA-QSA(P2PE), CTGA, CISSP, CISA | Principal
Tim Winston is a Principal Consultant in Point-to-Point Encryption (P2PE) and encryption key management at Coalfire Systems. Tim is an information security and risk professional with over 35 years of experience in all aspects of information technology. He has extensive experience in software development, networking, access control systems, identity management, cloud platforms, and has provided cyber security expertise to the largest cloud platform providers, payment terminal manufacturers, encryption service providers, payment service providers, government agencies, biomedical research organizations, healthcare solution providers, critical infrastructure providers, e-commerce service providers, and retailers.

Meg J Ray
Meg Ray is the Teacher in Residence at Cornell Tech. Meg is responsible for the implementation and design of the Teacher in Residence program, a coaching program for K-8 CS teachers in New York City schools. Meg served as a writer for the Computer Science Teachers Association K-12 CS Standards and as a special advisor to the K12 CS Framework. She is an experienced high school computer science teacher and special educator, and also taught graduate-level education courses at Hunter College. Previously, Meg directed the design of a middle school CS curricula. She researches CS teacher training as well as access to CS instruction for students with disabilities. Her work is published in academic journals and conference proceedings. She has a forthcoming intro to programming book aimed at middle and high school students. Meg holds a Master's of Science in Special Education from Hunter College and a Graduate Certificate in Blended Learning and Computer Science Instruction from Pace University.

CITATIONS

K–12 Computer Science Framework (2016). Retrieved from http://www.k12cs.org.

Maltese, A. V., & Tai, R. H. (2011). Pipeline persistence: Examining the association of educational experiences with earned degrees in STEM among U.S. students. Science Education,95(5), 877-907. doi:10.1002/sce.20441

Margolis, Jane. (2008). Stuck in the shallow end : education, race, and computing. Cambridge, Mass. :MIT Press.

Moakler, M. W., & Kim, M. M. (2014). College Major Choice in STEM: Revisiting Confidence and Demographic Factors. The Career Development Quarterly,62(2), 128-142. doi:10.1002/j.2161-0045.2014.00075.x

Pollock, L., Mouza, C., Czik, A., Little, A., Coffey, D., & Buttram, J. (2017). From Professional Development to the Classroom. Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education - SIGCSE 17. doi:10.1145/3017680.3017739

Wang, M., & Degol, J. (2013). Motivational pathways to STEM career choices: Using expectancy–value perspective to understand individual and gender differences in STEM fields. Developmental Review,33(4), 304-340. doi:10.1016/j.dr.2013.08.001

New Approaches to Cybersecurity Education (NACE) Workshop

What are some good ways to "future-proof" the education we provide?

Bridge Jobs (NICE Work Roles) and Course Offerings

There is an opportunity to measure the gap in program offerings and existing job functions by mapping the *NICE Cybersecurity Workforce Framework's* (NICE CWF) Work Roles to NSA/DHS National Centers of Academic Excellence in Cyber Defense (CAE CD) Focus Areas (FAs) or the more granular CAE Knowledge Units (KUs). This mapping will allow SFS to measure if there is sufficient coverage of the tasks, knowledge, skills and abilities for a given degree plan to allow a graduate to fill and succeed in a NICE Work Role.

Creating this mapping will highlight any gaps between CAE CD curricula and existing jobs. As Work Roles and Focus Areas are aligned, programs can offer students predefined *Plans of Study* (curricular paths) that are tied to a job function in the cybersecurity workforce. Maintaining this mapping will also provide an opportunity for programs to ensure that course offerings remain up-to-date with job offerings. As new NICE Work Roles and CAE Focus Areas are created and refined, this mapping will allow programs across institutions to adjust their course offerings accordingly and offer new *Plans of Study* where their courses offer the appropriate coverage. While this does not completely capture all jobs and roles in industry, it provides a starting point for institutions to measure "coverage".

Encourage External Learning Opportunities

Xavier Univeristy's Williams College of Business created a *Business Profession Passport Program* that "provides a structured way in which undergraduate students can gain knowledge, skills and networking contacts to complement their education and to educate them on the fundamentals of the working world [4]." This same concept and mechanism can be adopted for cybersecurity students. To account for the pace of change in cybersecurity, programs should consider creating a passport-like program that encourages students to go outside of their coursework and programs to seek out other opportunities, challenges and learning opportunities.

Programs can define specific activities or provide general categories, but the goal is to get students to seek out resources and opportunities that the program might not offer or does not have the capacity to offer in the near term (prior to the student's graduation). This passport concept also reinforces the importance of seeking out new opportunities and being in a mode of constant learning. Cybersecurity changes rapidly and, sometimes, at a pace faster than an employee's organization or student's program can adapt and marshal adequate training and resources to help the employee or student succeed. These activities might include:

- serve as an officer in a cybersecurity student organization or external organization
- obtain a certification (C|EH, OCSP, Security+, etc.)
- attend a conference, talk, colloquium or presentation
- create a presentation for a local businesses group around cybersecurity
- work with a local business to better secure their systems and assets or provide training
- co-author a paper with a faculty member
- create and maintain a security blog

- learn a new programming language
- complete an internship or co-op
- create and host a capture-the-flag (CTF) event
- create one or more demonstrations and presentations to teach fellow students and faculty a new skill or technology
- create a module or series of modules that can be incorporated into a new or existing course

Programs can modify the passport idea and attach "points" to activities based on difficulty or work-effort required to complete the task. Students could be required to earn a minimum number of points on their passport prior to graduation. Again, the goal is to supplement the coursework with other learning opportunities. Learning outcomes and objectives can be created in advance to tie the external learning opportunity with measurable outcomes.

Responding to Changing Workforce Demands

One of the benefits to using a *Plan of Study* for each student is the flexibility they offer. If courses are under development or are out-of-date, programs can adjust Plans of Study to provide students appropriate coursework that meets their educational goals. Additionally, programs can use the passport program, referenced above, to fill in gaps as curriculum is updated and developed.

Along with program flexibility, cybersecurity programs should look at the "Executive in Residence" model to help bridge gaps between industry and the classroom. For programs focused on producing graduates with more technical skills, development of a "Technologist/Specialist in Residence" might be more appropriate. Regardless of the terminology used, the goal is to bring in individuals working in organizations with experience using tools and techniques currently in practice. Programs can leverage these

individuals by having them teach and develop courses, mentor students, partner with industry, collaborate with faculty and provide input on curriculum.

Looking to bring in a technologist or executive would also allow the program capacity for development activities that both faculty and students could benefit from. Higher education focuses heavily on teaching and research and development should be added to the mix. The rapid pace at which technology changes may outpace what we research and teach and having a technologist may help a program grow new skill sets and expose students to new technologies not currently integrated into the curriculum.

Curriculum Development and Access to Resources

Should SFS institutions partner together to secure agreements with security and IT vendors to acquire software and hardware for use in course work and course infrastructure for a heavy discount or for free? Essentially create a *SFS School Consortium* whose members prioritize needed resources and work to secure those tools for students and faculty.

Lastly, SFS institutions should consider developing and using open-source courseware that maps to CAE KUs and CAE FAs. For institutions that have expertise in an area and have a quality offering, SFS students should have access to that content, regardless of where it is housed. Measuring quality and creating a platform to share courses would take time to spin up, but this would allow SFS students to leverage the best courses across the SFS ecosystem benefiting the SFS students' employers, too.

About the Author

Eugene Rooney is an Analyst/Programmer III and Adjunct Faculty member at the University of New Mexico's Anderson School of Management. Eugene earned a B.S. in Computer Engineering with a Minor in Economics and a MBA from the University of

New Mexico. Prior to his current role at UNM, Eugene worked at Century Link (formerly Qwest Communications), Sandia National Laboratories and UNM's Center for Development and Disability.

In his current role, Eugene provides reporting and forecasting for school leadership along with web application development and system administration duties. He was also actively involved in securing UNM's CAE-CD and CAE-R (re)designations the last 2 cycles. In his role as an adjunct faculty member, Eugene is looking forward to teaching *Windows Scripting and Automation (PowerShell)* and *Cybersecurity Competitions* in the Fall 2018 semester to undergraduate B.B.A. Management Information Systems (MIS) students and M.S. in Information Systems and Assurance (MS ISA) students.

References

[1] Baron, Ethan. "Executives-In-Residence: Filling A Business School Education Gap." Poets & Quants, Inc. May 2005. 12 April 2018 poetsandquants.com/2015/12/04/executives-residence-filling-business-school-education-gap/.

[2] Bennis, Warren, and James O'Toole. "How Business Schools Lost Their Way." *Harvard Business Review, Harvard Business Publishing*. May 2005. 12 April 2018 hbr.org/2005/05/how-business-schools-lost-their-way.

[3] "The Business Profession Passport." *Xavier University Williams College of Business*. 2017. 12 April 2018 www.xavier.edu/williams/business-profession/documents/Passport2017.pdf.

[4] "Business Profession Program." *Xavier University Williams College of Business*. 2018. 12 April 2018 www.xavier.edu/williams/business-profession/.

The Post-Millennials Have Arrived!

New Approaches to Cybersecurity Education

Julie A. Rursch

The Pew Research Center last month signaled that the post-Millennial cohort (born 1997-present) is the latest generation [1] we will need to adapt course content for in higher education. As compared the Millennial generation which experienced the Internet boom, the post-Millennials are "always on" and "always connected." Their world has always had access to social media and on-demand entertainment. Conversations can be held at any time, at any place, with anyone. These are the students we want to attract to fill cybersecurity careers.

One of the problems we have generally in education is, since many are likely part of the Boomer (born 1946-64) or Gen X (born 1965-80) generations, is that we teach linearly, processing one thing completely before moving on to the next while the Millennials (born 1981-96) and now the post-Millennials multi-task their thoughts and actions. As educators we have started to employ active learning activities in the classroom; think-pair-share (small group discussion), peer instruction exercises where one student is the "expert" and shares his/her knowledge with others. And, these activities work well in cybersecurity.

However, where we still are struggling is with providing students the ability to see how they can apply the skills being learned in the classroom, in the laboratory, and through homeworks in the after-college world. We know the post-Millennial generation is outcome-oriented. They need to be able to see the skills built through their classroom topics connect to future use of skills. Those of us who stand before them, construct the labs, and write the homework assignments tend to break the assignments and lectures into digestible pieces and forget to tie them all together with a final project or an overarching goal as we just work linearly through the week-by-week topics. We need to give students the bigger picture and help them see how the little part they are working on each week fits into their after-college goals.

As an example, let's look at developing a realistic, hands-on experience with SQL injections, the number 1 item on the OWASP Top 10 List, to provide personal experience and connections to the real world. As faculty we can easily demonstrate the SQL injection concepts in class, both in code and as an active demonstration. We can ask them on an exam how to prevent SQL

injections which should result in some answer like sanitizing, validating, and escaping the data. This works at Bloom's lowest level, knowledge. However, if we give them each a web server, tell them they are the administrator for that web site, and have them do both pentesting on their own server (so checking for all of the Top 10, network, and OS vulnerabilities), as well as a code review, they can more clearly see how the classroom experience ties to the after-college world. It also moves them into the application and sometimes analysis level of the taxonomy. I have had students tell me that they have had SQL injections demonstrated in a previous database class, but they never understood how to prevent it until they had the opportunity to try it on their own with their own web servers. And, if giving students the entire web site is too much all at once for the class level, we can start with code snippets that are contrived for the students' ease of learning and then use similar code in the overall web site to help them make the jump to the larger picture.

Similarly, giving students an entire network that is filled with vulnerabilities and letting them have the opportunity to evaluate, remediate, and then reevaluate gives them a realistic multiple machine environment in which to work. Again, there may have to be smaller pieces of the experience given to them at first and then give them the full network as a final project with similar problems. The point of both of these examples is to give them an experience that is as realistic as possible.

Further, every time a new topic is introduced in the classroom or lab a "current event" can be included. We seem to have no limit on real world cases to build our arguments. The perfect example this past semester was using Atlanta and their ransomware problems which not only allowed discussion of ransomware, but also discussion of good disaster recovery practices and the need for business continuity plans. The latter two are good business management practices that we don't always cover in cybersecurity courses. "Current events" can easily frame the week's topic in the classroom, lab, or homework.

Now, the realistic scenarios are difficult for faculty to generate and take a lot of time and energy. Likewise, faculty do not get rewarded for good teaching. They get rewarded for papers and conference attendance, even lecturers. So, there needs to be a shift in higher education to

value the realism added to the classroom and to recognize the demands post-Millennial students are making for this kind of classroom experience.

The second issue that we need to address is the adversarial feeling in cybersecurity curriculum. To date, many of the extracurricular activities, and to a lesser extent the hands-on activities in the labs or homeworks, tend to focus on an attack mentality. As an underrepresented population, whether gender or ethnicity or other, it can be hard to put yourself into that role. We are already in the minority and then to work with cybersecurity there is a certain level of bravado that occurs with competitions and events like capture the flag or build and defend events. Even seemingly innocuous things like rank ordering teams or people in event can reduce someone's self-efficacy and, therefore, their interest in cybersecurity. Additionally, when I have been in meetings where these kinds of objections are raised I was basically told the students (in the case I am thinking about, girls) needed to, "Toughen up, buttercup!" That is not an acceptable answer. We come at cybersecurity from many backgrounds and many experiences. We won't attract a diverse population if we are chastised for offering a different view.

Finally, there isn't enough reflection in current cybersecurity education. Even if we are doing a good job and providing post-Millennial students with outcome-oriented projects where they can build future use skills, we don't have them spend enough time thinking about how what they just completed related to their major, relates to career choices, and relates to what they need to improve upon. Simple reflection questions added into the weekly assignments that ask students to put what they just completed into the larger world context is also valuable in helping them understand the tasks role in the real world.

[1] M. Dimock. (2018, March 2). *Defining generations: Where Millennials end and post-Millennials begin*. Available: http://www.pewresearch.org/fact-tank/2018/03/01/defining-generations-where-millennials-end-and-post-millennials-begin/

Suggestions for Addressing the Changing Needs of the Cyber Security Workforce

Dr. Char Sample, & Dr. Connie Justice

Introduction

Cyber Security programs continue to expand across universities creating their own academic silos in response to growing workforce demands for cyber security professionals. Strong industry growth justifies this growth pattern in cyber security programs. These programs continue to turn out specialists that support the market demand.

However, a growing chorus have observed the need to break down silos, and are also calling for cross-disciplined approaches to solving cyber security problems (Peltsverger, 2015; Rowe, Lundt & Eckstrom, 2011; Crowley, 2003). Disciplines such as law, psychology, sociology, resilience, reliability, statistics, data science, international studies and others are becoming increasingly intertwined with cyber security (Ibid). The existent cyber security programs across accredited universities overwhelmingly continue to offer the same courses in penetration testing, policy, reverse engineering, risk, forensics, management and computer/network architecture; thus, Peltsverger's study of 2015 is still very applicable today.

In order to support the growing need for cross-discipline cyber security professionals, accredited cyber security programs will need to update their focus to not only embrace other academic disciplines, but also to understand how those disciplines can contribute to the improvement of cyber security and vice versa. A potential first step in this journey may begin with the offering of a security architecture course, where students are forced to acquire a cursory knowledge of other disciplines in creating a workable security solution.

Traditional architects combine knowledge from various disciplines in order to design structurally sound buildings (Savold, Dagher, Frazier, & McCallam, 2017). Similarly, security architects use skills learned in other disciplines to create robust network security solutions that support organizational goals. Creating strong defensive networks in support of a mission requires a mix of breadth and depth in the skill set of the network architect (Triolo, 2014).

Background

Academia silos exist because expertise is gained through research that focuses on a specific discipline while excluding others. Studies are purposefully tightly

restrained to allow the researcher to focus on a specific problem. Variables are limited, so that results or findings can be generalized for application where the same variables appear in different environments. Thus, cyber security would naturally follow the same structural pattern. This ultimately leads to cyber security professionals who are unable to effectively communicate with other groups in the workplace.

Cyber security programs have responded to industry's demand for skillsets. This approach showed initial successes. However, like nursing where professionals initially took care of patient's immediate needs, programs evolved to include increasing numbers of courses and disciplines (psychology, chemistry, sociology, kinesiology, etc.) in order better prepare nurses for their jobs. So too, cybersecurity curricula must evolve to include other disciplines with the goal of improving the students for the future workplace.

Cyber security is increasingly being asked to support other disciplines (law, finance, psychology, sociology, etc.) yet the programs are not reflecting this in their curricula. This failure to adequately support other disciplines further isolates cyber security professionals and may limit the students to becoming industry commodities. Commodities are quickly picked up and discarded this can be problematic for career growth.

These factors increasingly suggest the need to restructure cyber security programs away from the silo approach and into the cross-disciplined approach. The overall problem facing educational institutions, and students is that accredited programs may not adequately prepare their students for cybersecurity workforce challenges where diverse skill sets are becoming increasingly important. The general problem is the universities are focusing on technical rather than the holistic education of the cybersecurity learner when the workforce has a growing need for the holistic cybersecurity professional (Triolo, 2014).

Proposed Solutions

There are several potential solutions to the cyber security silo problem and each one warrants discussion. The proposed solutions are not limited to those discussed here and are likely highly situational. In some cases, some institutions may find some programs unworkable, for this reason these are suggestions not requirements.

1. Create a liaison position in the departments that interacts with other disciplines. This approach would entail hiring a liaison who reaches out to different

departments and works to define the necessary courses to make cyber security a joint major with the available disciplines.

2. Embed departments together for work on a common goal. An example of this approach occurs at Cardiff University in Wales where criminal justice, cyber security, data science, psychology, computer science exist in teams that work together in solving common research problems.
3. Require cyber security to be a dual major or joint major at the undergraduate level. This would force cyber security students to understand how cyber supports other disciplines and communicate with personnel in a manner that demonstrates an understanding of the discipline..
4. Create distinct curriculum for cybersecurity majors that include, but not limited to; cybersecurity risk assessment, creating policies, third party risk, and network security architecture.
5. Create cybersecurity curriculum for all disciplines to take before taking curricula in specific disciplines. See figure 1. Additionally, we could create common cybersecurity curriculum before discipline specific curriculum and midway or end of discipline specific curriculum, see figure 2.

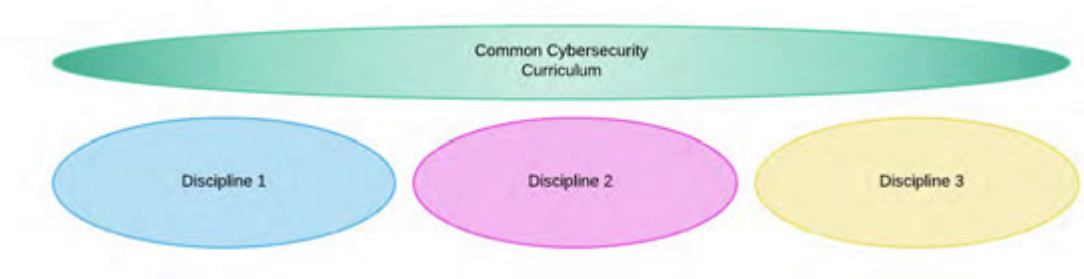


Figure 1: Common cybersecurity curriculum

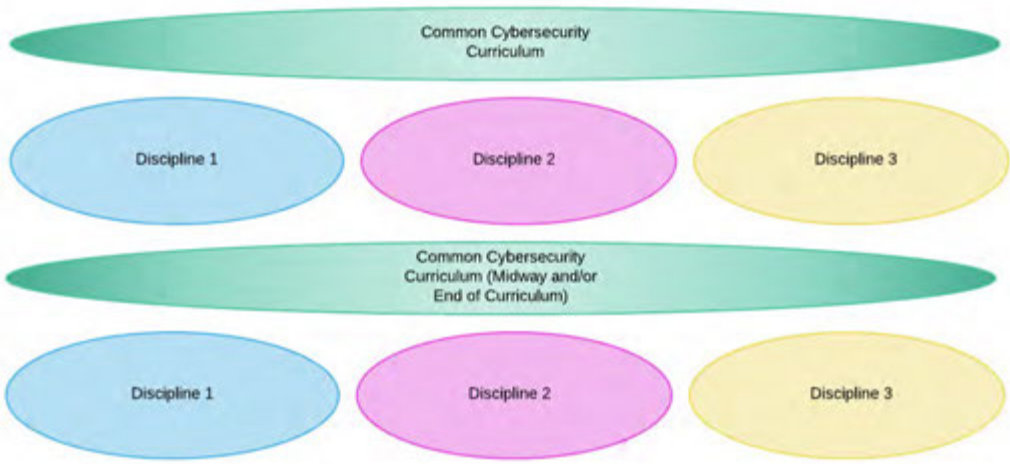


Figure 2: Common cybersecurity curriculum before and midway and/or end of curriculum

Specialized roles such as penetration testers and reverse software engineers provide an entry point into an organization, but generally speaking not professional growth opportunities Triolo (2014) noted that attackers need to be correct once and defenders need to be correct every time. A certain set of skills must bridge the gap between attacker skills and defender skills.

"Security architects design, build and oversees the implementation of network security for an organization" ("Become a security architect", n.d.). The security architect is entrusted to create a solution that reflects a deep technical knowledge of security products, and how to integrate those products in support of organizational goals. Solutions are complex and must work (Ibid). This mix of technical skills, management skills and people skills are unique. Introducing this mix of skills in cyber security programs as a foundational course would provide a foundation for a wider path of experiences for students and a potential bridge for those wishing to focus on policy.

Security professionals are frequently reminded to "bake in" security, not "bolt it on". This security by design must be engineered to the environment and processes that the security solution supports. Designing in security requires other disciplinary knowledge outside of the traditional technical areas.

Many universities and colleges participate in capture the flag cyber challenges that require participants to act as both attackers and defenders (Manson & Pike, 2014). These exercises are primarily focused on vulnerability exploitation, with prevention

being covered as a reaction to attack signatures (Manson & Pike, 2014). In some cases the cyber challenges require teams to build resilient solutions, but once again these solutions are designed to withstand known attacks in general. Creating and building of defences, in this arrangement, becomes an ad-hoc process that lacks rigor.

Conclusion

The changing nature of problems requiring cross-discipline approaches to cyber problems will force change in educational institutions programs. These changes will need to recognize the importance of other academic disciplines in creating the next generation of cyber security professionals. This paper put forth suggestions to offer potential ways forward.

References

Andel, T. R. and J. T. McDonald (2013). A Systems approach to cyber assurance education. *Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference.* Kennesaw GA, USA, ACM**:** 13-19.

Become a security architect. (n.d.). Cyber Degrees. Retrieved from https://www.cyberdegrees.org/jobs/security-architect/

Henry, A.P. (2017). "Mastering the cyber security skills crisis: realigning educational outcomes to industry requirements" ACCS discussion paper no. 4, August 2017, Australian Centre for Cyber Security, UNSW

Canberra, Canberra, viewed 26 Feb 2018, Available: https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/uploads/ACCS-Discussion-Paper-4-Web.pdf

Crowley, E. (2003, October). Information system security curricula development. In Proceedings of the 4th conference on Information technology curriculum (pp. 249-255). ACM.

Joint Task Force on Cybersecurity Education (2017). Cybersecurity Curricula 2017. Available: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Knapp, K. J., et al. (2017). "Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance." Journal of Information Systems Education 28(2): 101-113.

LeClair, J., et al. (2013). An Interdisciplinary Approach to Educating an Effective Cyber Security Workforce. Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference, ACM, (LOCATION).

Peltsverger, S (2015) "A survey of university system of Georgia cyber security programs" , Proceedings o the 2015 Information Security Curriculum,

Manson, D. and R. Pike (2014). "The case for depth in cybersecurity education." ACM Inroads **5**(1): 47-52.

McGettrick, A., et al. (2014). Toward curricular guidelines for cybersecurity. *Proceedings of the 45th ACM technical symposium on Computer science education*. Atlanta, Georgia, USA, ACM**:** 81-82.

Murphy, D. R. and R. H. Murphy (2013). Teaching cybersecurity: Protecting the business environment. *Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference*. Kennesaw GA, USA, ACM**:** 88-93.

NISTIR 8193 (DRAFT), National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators: Indicators for Performing Work Roles. (n.d.). Available: https://csrc.nist.gov/publications/detail/nistir/8193/draft

Ramirez, R. B. (2017). Making cyber security interdisciplinary: recommendations for a novel curriculum and terminology harmonization, Massachusetts Institute of Technology.

Savold, R., Dagher, N., Frazier, P., & McCallam, D. (2017, June). Architecting Cyber Defense: A Survey of the Leading Cyber Reference Architectures and Frameworks. In *Cyber Security and Cloud Computing (CSCloud), 2017 IEEE 4th International Conference* on (pp. 127-138). IEEE.

Triolo citation - https://www.scmagazine.com/hackers-only-need-to-get-it-right-once-we-need-to-get-it-right-every-time/article/537904/

Dr. Connie Justice
Department of Computer Information and Graphics Technology
Purdue School of Engineering and Technology
Indiana University Purdue University Indianapolis
cjustice@iupui.edu
317.278.3830

Dr. Connie Justice has over 30 years' experience in the computer and systems engineering field. Professor Justice is a Certified Information Systems Security Professional, CISSP. She created the networking and security options for CIT majors and a Network Security Certificate Program. She has designed and modified many courses in networking and networking security curriculum. Professor Justice is noted for her creation of the Living Lab, an experiential learning environment where students gain real world experience running an IT business.

Professor Justice takes extreme pride and is a great innovator in the area of experiential learning and service. Professor Justice has published several papers on creating course curriculum for information assurance and security. Professor Justice enjoys connecting students with industry projects that can provide them much needed hands-on experience.

Dr. Justice consults for and has managed IT departments in small, medium, and large sized businesses. She serves as Senior Security Advisor for a fortune 100 company. Her areas of research include: experiential and service learning, information and security risk assessment, risk management, digital forensics, network security, network and systems engineering, network and systems administration, and networking and security course development.

Dr. Char Sample

Dr. Char Sample is research fellow employed for ICF International at the US Army Research Laboratory in Adelphi, Maryland, and is also with the University of Warwick, Coventry, UK. Dr. Sample has over 20 years experience in the information security industry. Most recently Dr. Sample has been advancing the research into the role of national culture in cyber security events. Presently Dr. Sample is continuing research on modeling cyber behaviors by culture, other areas of research are information weaponization, data fidelity, and deceptive data.

Stephanie Siteman
Facebook InfoSec Diversity & Academia Program Manager
Proposal NACE

Stephanie Siteman is currently a manager at Facebook on the Cybersecurity Team. She handles all diversity and education initiative's that include curriculum, conferences, and direct relationships with education providers. She manages both domestic and global outreach projects and programs. She recently spoke at F8 about how to increase diversity in the workforce. She is passionate about making impact for the students, professors and universities.

1. What do we need to educate the next generation of cybersecurity & privacy specializes?
    a. We need to do a better job of bridging the gap between industry and academia by working closer together and learning from each other
    b. We need more quality hands on cybersec education available to the majority
    c. We need easier access to trainings and workshops and conferences
    d. We need diverse leaders and educators
    e. Change the way we think of cybersec
    f. Flexibility
    g. Sharing more best practices
2. How do we attract and educate a diverse set of students to succeed in a variety of national and private sector positions?
    a. Get leaders from both sectors to fully care and commit
    b. We need to make a clear and purpose effort
    c. We need to think differently
    d. We need to work with schools in the elementary schools and up
    e. We need to work with parents
    f. Diverse role models
3. What are some good ways to "future-proof" the education we provide?
    a. Plan to have the education dynamic and be flexible since security is ever-changing
    b. Create a roadmap and model as a foundation
    c. Find people who care and stick with them

Broadening and Diversifying the Reach of Cybersecurity Education

Abhilasha Bhargav-Spantzel, Principal Engineer, Intel Corporation
David Bills, Director of Academic Programs, Intel Corporation

Cybersecurity education is of prime importance in today's world. Increasing threats from attackers are motivated by financial and other gains, and these bad actors have access to advanced tools, resources and services from the hacker community.

This growing problem is evident in numerous news reports on the impact of cyber-attacks on individuals and organizations across the globe, and it will only get trickier as more digital devices and services become available in the future. These challenges, coupled with the shrinking talent base of solutions expertise, highlight the importance of broader cybersecurity education.

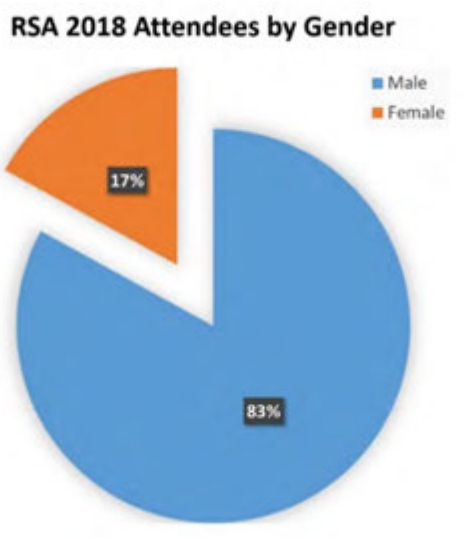
We need a comprehensive and granular approach. While no single individual is an expert in all cybersecurity areas, **foundational elements** can help provide the needed professional skills. This foundation should foster deep knowledge of the history and origins of cybersecurity challenges and solutions, as well as a good **understanding of their diverse range and interdisciplinary relevance**.

For decades, we've seen **significant research and security assurance initiatives**—from the U.S. Department of Defense Orange Book in the 1980's to the European Union's General Data Protection Regulation (GDPR) today. These efforts point to the network security protocols, system security design principles, privacy enhancing technologies, threat modeling, and other foundational elements for cybersecurity education. These must be coupled with an understanding of **today's compute platform**, not only **PCs** and **cloud** servers, but also internet of things (**IoT**) devices, connected **cars**, and the **ever-evolving world of digital services**.

This broader education effort must be grounded in how cybersecurity impacts us in both the **cyber and physical world**. The corresponding importance of **safety, privacy** and the **long-term consequences** to individuals and to society must also be considered.

To develop such a comprehensive approach, we need to nurture a diverse group of individuals—both teachers and students—to motivate and strengthen the defenses that become part of the design in every engineer's respective field. There is **no one-size-fits-all to attract the diverse set of individuals,** so one must **employ targeted tactics to attract** specific groups of **individuals.**

The lack of diversity evident at RSA-2018, where women comprised only 17 percent of attendees, points to a problem that needs to be tackled**. "Failure of imagination**" has been cited as the reason we were caught off-guard by the Russian interference with the 2016 U.S. presidential election, and the same was said about Sept. 11, 2001. By bringing more types of



people with a more diverse range of experiences and backgrounds into protecting our security, we can broaden the imagination brought to bear on future threats, especially in the cybersecurity domain.

We as society have yet to understand the full impact and cost of decisions made yesterday, today regarding **privacy**. We must think this through completely and how it will **impact our future** and the future of generations to come. If we are not careful, we will see our **technologies weaponized** which makes nuclear warfare obsolete. A scary proposition!

Finally we need to **future proof** our education system. The **education system** has never moved at the **speed of technology** and business and this must change. Education must have **a sense of urgency** and move at a faster pace. As part of growth mindset – we need to get out of the old mentality of how school is run. One way is to **partner with industry** to understand the pain points and quickly **develop the curriculum to bridge the gap**. **Education meets real-world experience and moves at the speed of business**. This has to be tackled carefully to **avoid "shiny object syndrome"** and ensure the due diligence is done to tackle the underlying problem. The education goes both ways, similar to many feedback loops in carefully designed security and risk management systems to allow continuous education opportunities for all.

It is great to see strong cybersecurity education efforts by notable leaders academia, government and industry. For example, Intel is leading initiatives with the academic community to bring diversity to high-tech in general and cybersecurity in particular. We focus on **outreach programs** to universities and students of **all genders, backgrounds, interests** and various majors to talk about the comprehensive cyber security considerations.

Training cybersecurity professionals is now more critical than ever. A recent government and industry Task Force is predicting that 1.8 million cybersecurity-related positions worldwide will go unfilled by the year 2022. Building collaborative programs and ensuring diversity of representation in these programs would be critical in **addressing this shortfall** in needed professionals to tackle the challenges and **win on our path ahead.**

Abhilasha Bhargav-Spantzel is an Intel Principal Engineer focused on identity, security and privacy. She has numerous patents and broad experience in identity management, cryptography, biometrics, hardware devices and system security. She leads multiple diversity and inclusion efforts at Intel, and actively drives development of women in engineering and cyber security. Find her on LinkedIn.

David Bills is the Director of Academic Programs for the Platform Security Division where he collaborates with academia to drive security research, education, and talent acquisition. For the past 2 years, he has served on Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS) board. David built Intel's scale ISV software enabling ecosystem from prior to his academic work. LinkedIn

The need for a National Cyber Academy:
The United States Cybersecurity Academy

In the 21st century, the landscape for war has extended from land, sea, air, and space to a fifth domain- cyberspace. America's digital strategic infrastructure is now considered a "strategic national asset" and protecting this has become a national priority. The state of cybersecurity for the nation has reached a critical status. There is an urgent need for skilled cybersecurity professionals across the workforce and for leaders in the federal government, across the security agencies. The National Science Foundation's Scholarship for Service program is one vehicle geared towards encouraging the best cyber talent to work for the government, at least for several years, before being lured to industry for higher salaries. This program has encouraged many students to work for agencies such as NSA, CIA, etc.

The cybersecurity crisis requires a multifaceted solution and the time is right for another service academy focused in cyber. Dr. Mark Hagerott and Admiral (Ret.) James Stravridis formally recommended this in March 2017 in their Foreign Policy article entitled "Trump's Big Defense Buildup Should Include a National Cyber Academy." Additionally, Dark et al. propose the idea in the 2018 CISSE paper entitled: The Cyber Cube: A Multifaceted Approach for a Living Cybersecurity Curriculum Library.

There is a history for this. After the Revolutionary War, soldiers and legislators, including Washington, Hamilton and John Adams, concerned about American reliance on foreign engineers and artillerists, lobbied for the creation of an institution devoted to the arts and sciences of warfare. In 1802, Thomas Jefferson signed legislation to establish the United States Military Academy at West Point, a strategic military center. In addition to providing military officers, the USMA became the first accredited civil engineering school and its early graduates helped construct the nation's first railway lines, bridges, harbors and roads. The mission of the USMA is: "To educate, train, and inspire the Corps of Cadets so that each graduate is a commissioned leader of character committed to the values of Duty, Honor, Country and prepared for a career of professional excellence and service to the Nation as an officer in the United States Army."

Similarly, the United States Naval Academy was founded in 1845 in response to a need for trained officers at sea. The curriculum of the USNA has shifted to accommodate the high tech fleet of nuclear-powered submarines and surface ships and supersonic aircraft .The USNA, located in Annapolis, MD, states the following mission – "To develop Midshipmen morally, mentally and physically and to imbue them with the highest ideals of duty, honor and loyalty in order to graduate leaders who are dedicated to a career of naval service and have potential for future development in mind and character to assume the highest responsibilities of command, citizenship and government."

Most recently, the Air Force academy was built to address our needs in aerospace including missiles and atomic weapons. Following decades of political pressure to increase America's air power, it was not until 1954 that President Eisenhower (ATC) initiated a detailed curriculum for the Academy program. The United States Air Force (USAF), formed as a separate branch of the U.S. Armed Forces in 1947, is the aerial and space warfare service branch of the United States Armed Forces. The Air Force defines its core missions as "air and space superiority, global integrated ISR, rapid global mobility, global strike, and command and control." While each of the military academies have their own cyber programs, their primary aim is to provide officers to their respective military branch. The numbers are relatively small - the USMA produces 15 graduates per year and the USNA's freshmen class has 110 cyber operations majors (the class of 2018 had 22 cyber majors). While some service academy graduates eventually work for the federal agencies, generally this is after they have completed their service requirements.

The defense and military landscape has changed, and the nation's infrastructure and public safety are at stake. The United Stated Cybersecurity Academy (USCA) that produces the much-needed cyber specialists for the federal government would bolster the status of the US in the international arena and help protect our critical infrastructure. Additionally, the USCA would provide a center or hub for the cybersecurity community and foster synergistic activities, such as workshops, training, lectures, competitions and other cyber events, to vitalize national workforce development.

The USCA would in many ways resemble the existing academies, accredited, free, and selective, but graduates would be required to serve as civil servants for the federal government. The cybersecurity major could resemble the NSA cyber Ops program, be deeply technical, and include computer science, cybersecurity offense and defensive skills as well as a solid liberal arts courses including history, government, and cyber laws. Given the technical landscape, the USCA

should be adaptive and include significant virtual infrastructure to allow cybersecurity leaders and experts across the world to provide instruction remotely. The faculty of the USCA would not be tied to the traditional doctoral requirement as for most four-year schools, but instead facilitate the cybersecurity experts in the country to serve as faculty. Additionally, the entrance requirements would allow for students with disabilities. A prep school or ROTC program geared towards cyber would be a good complement, perhaps following a model as being kicked off in Huntsville Alabama.

Obviously, the costs for such a brick and mortar institute are high, so I propose that the academy begin as a virtual infrastructure, including a "national credit" model where the USCA offers full courses in critical areas such as reverse engineering and cyber operations. National credit would allow schools that are trying to build cyber programs supplement their programs by accepting the USCA courses for credit. The academy should include a library of cybersecurity resources for K-20, including curriculum that is mapped to national standards and aligned to learning taxonomies, including labs and exercises and different modes of instruction. Additionally, a cyber range, both public and private, is necessary to support the academy and the digital library. Given the national shortage of cybersecurity faculty, this would help better prepare the cyber workforce.

In addition to start-up and operating costs, another significant challenge to a national cybersecurity academy is diversity. Since women were permitted to enter the military academies in 1975, each of the academies have worked hard to achieve diversity and each has struggled against perceptions of hostile environments. The USCA must be created with an eye towards fostering diversity, not only for women but across ethnicity, to provide an inclusive environment. Socialization and courses on inclusion and acceptance would be key to producing cyber leaders with these attributes.

Cyberspace is the new battlefield. It is imperative that the United States prepare for it on all fronts.

Luis M Vicente
Associate Professor, Associate Director,
(ECECS) Electrical, Computer Engineering and Computer Science Department,
Polytechnic University of Puerto Rico (PUPR)
377 Ponce de León Ave, Hato Rey, PR 00918
(787) 622-8000 Ext. (340) / Fax: (787) 281-8342

Personal address:
131 Calle Portugués, San Juan, PR 00926
lvicente@pupr.edu ,1-787-217-4563

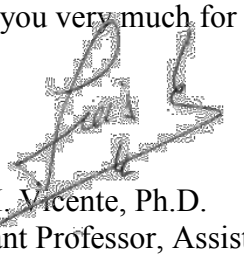
Dear organizers of the 2018 NACE Workshop,

This is Luis Vicente, faculty member of the Polytechnic University of Puerto Rico (PUPR). I am writing you this letter because I would like to participate in the NACE Workshop, on June 9-10, 2018 in New Orleans, LA. PUPR is a National Center of Academic Excellence in Information Assurance Education (CAE/IAE) and we are devoted to graduate students proficient in Cybersecurity among other fields.

I am part of the PUPR faculty as Associate Professor, Associate Director of the ECECS Department. My main interest attending this workshop is to learn about new Cybersecurity trends, how to efficiently teaching these topics to our students. Also, find about funding, educational, and professional opportunities for our Hispanic students in Puerto Rico. Here at the PUPR most of our faculty and almost 100% of the students are from Hispanic minorities. However, since Puerto Rico is a US territory we all hold US citizenship. This put our students in a very advantageous potential position of being able to work anywhere in the USA, including classified jobs. Last but not least, I would like to increase the underrepresented Hispanic group in the Cybersecurity and National Security fields. The reality is that our minority is not fully represented in those areas yet.

Please find attached a short bio sketch, and a paper intended to inspire thought and discussion about the field of Cybersecurity.

Thank you very much for your attention.



Luis M. Vicente, Ph.D.
Assistant Professor, Assistant Director ,
Electrical, Computer Engineering and Computer Science Department,
Polytechnic University of Puerto Rico,
377 Ponce de León Ave, Hato Rey, PR 00918
(787) 622-8000 ext (340) / Fax: (787) 281-8342 / lvicente@pupr.edu

Dr. Luis M Vicente is the associate director and associate professor of the Electrical & Computer Engineering and Computer Science Department at the Polytechnic University of Puerto Rico. He received Ph.D. in Electrical and Computer Engineering at the University of Missouri-Columbia in May 2009 where he already was author or coauthor of five publications.

From February 1990 to February 2003, Dr. Vicente worked in industry. First, in the Military-Aerospace Division, SENER Group, Spain. In addition, he worked with Voyetra Inc., New York, and with SIEMENS Corp., Madrid.

From February 2003 to June 2009, he became Assistant Professor at the Polytechnic University of Puerto Rico (PUPR). In 2009, Dr. Vicente was promoted to Associate Professor and Mentor of the Master Program in Electrical Engineering at the PUPR. In 2011, he was appointed Sponsor Research Office Coordinator.

In 2012, he was promoted to Associate Director. His research interests include beamforming, array processing, statistical signal processing, adaptive filters, High Performance Computing on Signal processing, and Cybersecurity. As a graduate thesis advisor, he already graduated fifteen students in the digital signal processing area, high performance computing and parallel processing. He is now pursuing a Graduate Certificate in Digital Forensics, expecting to be completed in fall 2018.

Cybersecurity permeates all aspects of our society. It is well known that every electronic equipment connected to the web is susceptible to be hacked, spied on, and the probability of that happening is almost one hundred percent. If that is so, why people are still in negation? What is the reason Cybersecurity is not already part of elementary courses in Engineering? Or even more, why is not taught in every high school in our country, at least at the basic level?. It seems we only pay attention to Cybersecurity after we have been victim of a cyber-crime. We need to change that into a proactive measure!!

The first measure to arm ourselves against cyber-crimes is to be aware of its reality. Learn the basics and at least have a true knowledge of what are the risks we are taking when going online. Getting involved in Cybersecurity is not difficult at all. To have a basic knowledge of how viruses work, how to protect ones computer and smartphones could be learned for people with less than high school academic level. Almost every one of us know what is an anti-virus, a virus, have some ideas of Trojan horses and such. However, all this knowledge usually comes to us from not verifiable sources, like Facebook, personal blogs, unverifiable web pages, gossip. It would not be better to acquire this knowledge from verifiable, academic sources? Why not be learned in schools by adequate teachers in the area? Why not learn all the topics in their correct order and with a strategy in mind? These concepts do not require advanced mathematical skills. These advanced mathematical skill are only needed if you really want to have a deep knowledge of some areas, for example, in cryptography.

Recently, some universities are paying more attention to the importance of Cybersecurity, and not only Engineering universities, but also universities devoted to law. From Chuck Easttom book Computer Security Fundamentals, we read that the University of Dayton School of Law has an entire website dedicated to cyber-crime. The university has extensive links on cyber-crime, cyber stalking, and other web-based crimes. As we all move forward into the twenty-first century, we should expect to see more law schools with courses dedicated to cyber-crime.

I propose to encourage the teaching of some basic topics in Cybersecurity at the very high school level, or even earlier. Starting with the concept of networking layers. To have at least the awareness that all our communications are structured in OSI layers. Then, teaching the students how the

hackers use these layers to infect the network with malware. In addition, a basic knowledge of all kind of malware should be part of the class. The difference between virus, worms, Trojan horses, among other. In addition, chapters on anti-virus, firewalls, anti spyware, would be needed to have a global idea of the basics of Cybersecurity.

None of the above would permeate the mind of our young students without some hands-on laboratories. I propose the creation of some basic laboratories where the students could implement and connect a small network. Both wired and wireless. To acquire the basic knowledge of how it works and how the devices communicate with each other. In addition, some testing, penetration testing, and vulnerability testing. All inside a controlled laboratory network of computers. Create contests where some students would be the defensive barrier of a network and other students to be the cyber attackers.

One of the main difficulties in making reality above ideas is the assumption that all knowledge acquired by our young students could be used for criminal purposes. I am against that idea when referring to our American joung students of at least 16 years old. Let's think for a moment what is the minimum age for americans to use and practice with a long shot gun. Just a look at a Washington Post article (By Roberto A. Ferdman and Christopher Ingraham August 27, 2014), we learned that in 30 states there is no minimum age. To me it does not seem a great idea to give a gun to a children, but if we think of young students, around 16 years old. Should we prohibit the knowledge of guns because they could be potential criminals? It is not true that they could learn the topic form the internet, and not precisely by the best people to teach how to use, and the risk of using them? Let's make another analogy. Sex. Why is necessary to teach youngsters about sex? We all know why. However, sex has been a taboo for centuries. Nobody would want to talk or even teach about it. Now, what is the trend today about sex? Why it should be different with Cybersecurity? It is not better to teach all aspects of Cybersecurity in our controlled schools, to young people of at least certain age, than for them to learn from real criminal hackers posting tutorials in the web, and performing penetration testing on the neighbor Wi-fi access point?

We know in conferences and workshops when the speaker ask if your company has been hacked, not everybody wants to disclose that. It seems is shameful to be a victim of cyber-crime. Not

everybody wants to admit they have been victims of a cyber-crime. Cybersecurity is our present time taboo. However, we know by experience in other areas of our life that is better to have good basic knowledge of certain topic than to ignore it or even learn it from the wrong teaching channels. We need a paradigm change in order to place Cybersecurity in its own level of importance.With the fast trend of newer technologies, even faster than ever, we have to admit that the level of importance is rather high. We need to be prepared, armed and ready to know, and defend ourselves against the risks of using technology. We need to prepare our American students to join the good guys.

Regarding the question of how do we get more US citizens, and a more diverse population, into cybersecurity in meaningful ways? I could answer this from our little Caribbean island of Puerto Rico. From centuries, this has been a land of pirates, buccaneers, and smugglers. Even today, the black market, narco-activity, violent crime on our small island streets is rampaging. There is not a single family in the island where that kind of violence did not touch in one or another aspect. On one hand, it is not difficult to convince our young people to join the bad boys, fast money, fast life, short life. However, here in our universities, we are given them sanctuary and teaching them to arm themselves against that kind of life. We teach them how to outsmart the bad people using the latest technology available. We give them power. As I stated in my presentation letter, PUPR is a National Center of Academic Excellence in Information Assurance Education (CAE/IAE) and we are devoted to graduate students proficient in Cybersecurity among other fields. This is a challenge that any smart student would take, making them truly heroes!!. To outsmart the bad people and to contribute the goodness in this island is something not easily understood for people that did not suffer the violence of our streets. For young Puerto Rican students that have seen real suffering, to become proficient in an area where they feel they can contribute to goodness is a true mission. Most of our graduated students are working for security agencies in Washington. They are proud and they make us proud. We have more motives to anyone to help our young students from the beginning of their academic life to learn Cybersecurity. And, we are committed to do so.

Take a Long View: Integrate Security Topics into ALL Software Development Education

The software development community does a lousy job of delivering software that minimizes the attack surface. In the National Vulnerability Database [8], an exact match search on the keyword Microsoft identifies 275 records for the last 3 months. A similar search on the keywords Linux and Oracle identifies 218 and 326 records, respectively, for the last 3 months. Neither proprietary nor open source software are immune from bad or ignorant secure software development practices. This situation is not new. In the SANS report on the Top 25 Software Errors [10], the current list identifies 16 errors that also appeared in the 2010 list.

Our current state of ineptitude is even more perplexing when one considers that two researchers published eight security principles in 1975 [9], over forty years ago! Five more security principles were described in 2013 [7]. Why aren't these thirteen security principles - economy of mechanism, fail-safe defaults, complete mediation, open design, separation of privilege, least privilege, least common mechanism, psychological acceptability, secure the weakest link, defend in depth, be reluctant to trust, promote privacy, and use your resources – discussed and practiced in all undergraduate curricula that has a role in software development?

There appears to be some positive momentum in emphasizing secure software development in undergraduate computing programs.

The most recent computer science undergraduate curriculum guidelines (CS2013) represents the first time security was recognized as a separate knowledge area with the inclusion of Information Assurance and Security [1]. The most recent software engineering and information systems undergraduate curriculum guidelines - SE2014 and IS2010, respectively - have significantly increased the visibility of security.

The current CISO of Turner Broadcasting System is calling for a “moonshot to reestablish our digital strength (via) a profound, coordinated effort to bolster our cybersecurity systems and protect our democracy from hackers” [3]. In his book, Chronis draws inspiration and lessons learned from other moonshots – getting a man on the moon, defeating fascism, and eradicating polio. One of his pillars for fixing cybersecurity is to minimize software vulnerabilities through better software development practices, market incentives that provide more information to consumers about the safety and security of products, and software

technologies that make it easier to identify/fix security defects (e.g., self-healing code, deep learning platforms).

It is clear that both educators and industry see the need for vast improvements in how we develop software. The question becomes, how do we cover security topics in our computing-based programs so that we have the greatest impact on the next generation of information technology leaders? While this question pertains to the three curriculum guidelines (CS2013, SE2014, and IS2010) most directly related to software development, only the CS2013 perspective is described below.

One option is to create a separate computer science course that covers cybersecurity. Assuming CS programs make this course a requirement and not an elective; this would likely improve students understanding of security topics and their use in software development. Another option is to integrate security topics into the entire CS program. This is what we have done in our INCUBATE project [4, 11]. One example of this integration is in our CS1 course, where we introduce security principles (e.g., CIA, anonymity, authentication, assurance, and non-repudiation) and input validation, with hands-on exercises that ask students to apply various types of input validation checks. While our assessment results to-date are positive, our first cohort of students that will have experienced four years of integrating cybersecurity topics into CS will graduate in May 2019. While we expect assessment results to be positive for this cohort, the full impact of our efforts will be unknown for at least another 5-10 years, or until these students have gained enough work experience to influence the culture within their respective organizations.

Changing the culture of the software development industry to adhere to security policies and to apply security controls and mechanisms will take time. Perhaps twenty years from now, when current college students start to take on leadership positions, we will see results of the educational decisions we make over the next few years.

Diversity of Thought: Social and Political Perspectives on Cybersecurity

Since technology has created our cybersecurity problems, technology can solve these problems. This thinking is shortsighted because it ignores the fact that humans develop and use these technologies, and humans are the source and target of cybersecurity attacks.

Having students study the social sciences as part of a cybersecurity program provides these students with other ways of thinking about the issues that confront us. A workshop on social science, computer science, and cybersecurity held in 2013 [5] had as its goal to develop communities of researchers from social science and technology fields that cooperate in the development of new and improved cybersecurity systems. In the summary report from this workshop [5], white papers written by the attendees provide their perspective on the workshop goal. The following quote exemplifies the workshop discussions in support of the need for educational opportunities that blend social sciences and information & system security technology.

> "The fact that humans from several different walks of life are interacting with these systems on a daily basis has prompted a paradigm shift: rather than designing secure systems with arbitrarily defined use models, we must design secure systems with use models informed by how people interact with each other, computers, and information. This security paradigm necessitates a close collaboration between technical and social scientists so that the design of secure systems incorporates an understanding of the needs and capabilities of the billions of people that will rely on them." (Page 28, Chris Kanich, Computer Science Department, University of Illinois at Chicago.)

In addition, a 2014 paper published by the National Council in the Social Studies [2] includes the following quote.

> "… the disciplines of the social sciences promote ways of knowing and deliberating about data and information that are critical to policy development and the implementation of cybersecurity initiatives. Building the capacity of the next generation of social scientists to tackle these emerging issues is imperative."

While Chronis [3] believes that minimizing software vulnerabilities is crucial to his cybersecurity moonshot, the other pillars of his moonshot relate to social and political perspectives. His other pillars: educating everyone about social engineering attacks; federal government leadership in the form of regulations and incentives; and better corporate governance of their cybersecurity programs.

Le Moyne College launched a new cybersecurity undergraduate program in fall, 2017 developed by faculty in anthropology, computer science, criminology, political science, and sociology [6]. This program has used the Catholic Jesuit mission of *educating the whole person* as motivation for *educating the whole cybersecurity professional* with perspectives in: crime, society & culture; information & system security; and policy & law. Our thinking in developing this new program is to position our students for success in a variety of career paths, some of which may have an ancillary relationship to cybersecurity.

Bio Sketch

David Voorhees is an associate professor of computer science at Le Moyne College. He is the director of the computer science, software applications and systems development (i.e., a software engineering program), and cybersecurity undergraduate programs. Dave worked for 19 years in industry before starting as a visiting assistant professor at Le Moyne in August 1999. He earned his Ph.D. in computer science from Nova Southeastern University in 2005. Dave is the PI of the NSF-funded INCUBATE project briefly described in this paper.

References

[1] ACM, (2018). *Curricula Recommendations*. Retrieved April 29, 2018 from https://www.acm.org/education/curricula-recommendations.

[2] Berson, M. J., & Berson, I. R. (2014). Bringing the Cybersecurity Challenge to the Social Studies Classroom. *Social Education (National Council for the Social Studies), 78(2), 96-100*.

[3] Chronis, P.K. (2017). *The Cyber Conundrum: How do we Fix Cybersecurity?.* CreateSpace Independent Publishing Platform.

[4] Das, A., Voorhees, D., and Choi, C. (2018). *INCUBATE: Injecting and assessing cybersecurity education with little internal subject matter expertise*. Retrieved April 29, 2018 from http://research.lemoyne.edu/incubate.

[5] Hofman, L. J. (2013). Social Science, Computer Science, and Cybersecurity, Workshop Summary Report. Cyber Security Policy and Research Institute, The George Washington University, Report GW-CSPRI-2013-02 retrieved on October 21, 2016 from https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/Final+08+22+13+1301+Report+Social+Science.pdf.

[6] Le Moyne College Catalog, (2018). *New Cybersecurity Undergraduate Program*. Retrieved April 29, 2018 from http://collegecatalog.lemoyne.edu/arts-sciences/cybersecurity/.

[7] McGraw, G. (2013). *Thirteen principles to ensure enterprise system security*. Retrieved on July 28, 2015 from searchsecurity.techtarget.com/opinion/Thirteen-principles-to-ensure-enterprise-system-security.

[8] NIST, (2018). *National Vulnerability Database*. Retrieved April 29, 2018 from https://nvd.nist.gov/vuln/search.

[9] Saltzer, J.H. and Schroeder, M.D. (1975). The Protection of Information in Computer Systems. In *Proceedings of the IEEE, 63(9)*.

[10] SANS, (2018). *CWE/SANS Top 25 Most Dangerous Software Errors*. Retrieved April 29, 2018 from https://www.sans.org/top25-software-errors/archive/2010.

[11] Voorhees, D. and Das, A. (2018). Injecting cybersecurity into a CS program: a non-specialist perspective. *Journal of Computing Sciences in Colleges, 33(6)*.

Junior Cyber Corps

Introduction

Cybersecurity is critical to the national security and economic prosperity of the U.S. By many accounts, there is a severe shortage of trained cybersecurity professionals to meet the current demand in industry, academia, and government. Cyberseek.org currently estimates the shortage at 285,000. Other studies provide estimates that range far higher. These estimates also assume a minimum of a 2 year degree in cybersecurity, a four year technical degree with a cybersecurity focus, and/or cybersecurity certifications such as CISSP, Certified Ethical Hacker, and Security+ to name a few.

Colleges, universities, and other post-secondary education can't solve the problem alone. They are already serving as many applicants as they can and the need for additional faculty at these levels is now becoming a demand. There are programs in place to grow the post-secondary education capacity. Yet even these measure are not projected to meet the growing demands of employers. As this new capability comes online, it is not clear there will be enough interested and qualified students to make effective use of it, thus creating a likely shortage of students applying to participate in cybersecurity programs at the post-secondary level.

We have both an absolute shortage of students applying, and few of those applying are as prepared as they could be with minimal involvement from primary and secondary educators. We need more students interested in and prepared to pursue post-secondary education in cybersecurity.

To address this shortage will require primary and secondary school students to be more knowledgeable about cybersecurity principles and about the wide variety of career opportunities in cybersecurity. We propose a combination of in-school and

extracurricular activities similar to a Junior Reserve Officer Training Corps (JROTC), named something like Junior Cyber Corps.

Junior Cyber Corps

A junior cyber corps is proposed to introduce primary and secondary school students to the field of cybersecurity, as it applies across the many disciplines that it touches (e.g., ethics. law, business, IT, computer science, engineering) and the “soft skills” (e.g. communication skills, people skills, leadership skills). The junior cyber corps will not only introduce foundational knowledge as it relates to these disciplines, but will also introduce students to the career opportunities that exist, along with the pathways that are available to them to take towards these careers.

Such programs could vary in intensity from extracurricular clubs to significant components of a military school or many points in-between. Such variety could require as little as a STEM-capable member of the community willing to volunteer to be a club mentor or a teacher taking on coach-like responsibilities, all the way up to a dedicated staff supporting an entire curriculum.

The cyber corps programs would include in-school classes, after school clubs, competition teams, seminars/tutorials/conferences, and mentoring from cybersecurity professionals.

-- National Cryptologic School, College of Cyber

Encouraging Primary & Secondary School Teachers

Introduction

Cybersecurity is critical to the national security and economic prosperity of the U.S. By many accounts, there is a severe shortage of trained cybersecurity professionals to meet the current demand in industry, academia, and government. Cyberseek.org currently estimates the shortage at 285,000. Other studies provide estimates that range far higher. These estimates also assume a minimum of a 2 year degree in cybersecurity, a four year technical degree with a cybersecurity focus, and/or cybersecurity certifications such as CISSP, Certified Ethical Hacker, and Security+ to name a few.

Colleges, universities, and other post-secondary education can't solve the problem alone. They are already serving as many applicants as they can and the need for additional faculty at these levels is now becoming a demand. There are programs in place to grow the post-secondary education capacity. Yet even these measure are not projected to meet the growing demands of employers. As this new capability comes online, it is not clear there will be enough interested and qualified students to make effective use of it, thus creating a likely shortage of qualified students applying to participate in cybersecurity programs at the post-secondary level.

We have both an absolute shortage of students applying, and few of those applying are as prepared as they could be if there were but minimal involvement from primary and secondary educators. We need more students interested in, and prepared to pursue, post-secondary education in cybersecurity. This can only be accomplished by their teachers introducing them to cybersecurity concepts prior to post-secondary school.

To address this shortage will require primary and secondary school teachers to be more knowledgeable about cybersecurity and career opportunities in cybersecurity. We propose a multi-pronged approach:

1. Increase the cybersecurity resources available to teachers during their college experience as well as part of their continuing professional development.

2. Provide incentives for teachers to gain cybersecurity expertise and share it with their colleagues and students.

Increased Cybersecurity Teaching Resources

Teacher education programs need access to better materials and subject matter experts in order to provide new and existing teachers with the cybersecurity knowledge they need. We believe that a grant program which brings Education departments together with Computer Science/Computer Engineering departments for the purposes of creating and sharing materials for new and existing teachers is needed. Further these same teams should be encouraged to develop materials the teachers can use (and other existing teachers can use) in their primary and secondary school classrooms.

Quality and effective cybersecurity teaching resources developed with these grants should be made available to all primary and secondary educators via a mechanism such as a digital library. Keys to a successful digital library include: being easily accessible, a broad collection of quality and effective materials, robust search capabilities, and continual maintenance of materials and the library itself. While such a digital library should not be run by the federal government, the creation and maintenance of such a library could be seeded with an investment from the federal government.

Further, since the most effective learning often takes place through hand-on experiences, many schools with only rudimentary computer support would benefit from access to a remote virtual training environment or laboratory. While such a training environment should not be run by the federal government, the creation and maintenance could be seeded with an investment from the federal government.

Simply educating new teachers while they are in college is not sufficient. First, this would only reach new teachers and thus greatly limit the growth of informed teachers. Second, the rate of change in cyber security requires refreshing teachers after a few years. Thus, much of the cybersecurity material developed above must also be suitable for use in professional development environments in which existing teachers regularly participate outside of the university or college. Therefore, we recommend the above grant program include grants to create and maintain certificate and badging programs consistent with state guidelines for continuing teacher education and licensing.

Teacher Incentives

The demands upon primary and secondary school teachers is already extraordinary. Simply adding to their to-do list with additional tasks or giving them additional cybersecurity choices will not be enough to achieve the level of engagement that is required. Incentives aimed at individual teachers will be needed. Such incentives should reward both cybersecurity learning as well as passing on that learning to colleagues and students. Possible incentives may include:

- Subsidizing student tuition for cybersecurity-related courses in an Education program in order to make such electives more attractive
- Expanding the Scholarship for Service program to include teachers graduating with a cybersecurity certificate
- Creating free or low-cost cybersecurity-related professional development opportunities for existing teachers

- Forgiving portions of student loans for teachers that achieve cybersecurity-related achievements (e.g., coach winning Cyber Patriot team; earn cybersecurity-related certifications; winning competitive award for cybersecurity-related activities; running successful, cybersecurity-related professional development event in their school)
- Providing tax incentives for companies that offer paid summer positions, like internships, in cybersecurity-related jobs designed for teachers, to give them both deeper cybersecurity knowledge and, more importantly, information on careers in cybersecurity to share with their students.
- Encouraging federal government agencies and departments to offer paid summer positions, like internships, in cybersecurity-related jobs designed for teachers, to give them both deeper cybersecurity knowledge and, more importantly, information on careers in cybersecurity to share with their students.

Conclusion

We face a critical shortage of trained cybersecurity professionals. This shortage is affecting both government and the private sector. The demand for these professionals is growing much faster than the nation's capacity to train new professionals. To date, our efforts to address the problem have focused upon post-secondary and workplace training. These programs will run short of qualified entrants if we don't include primary and secondary school in the solution and that begins with developing a cadre of informed teachers in those schools. The federal government must invest its resources in this community.

-- National Cryptologic School, College of Cyber

CS4A: A New Approach for Cybersecurity Workforce Development

Yong Wang
Beacom College of Computer and Cyber Sciences
Dakota State University
Madison, SD
yong.wang@dsu.edu

Abstract

The paper proposes a new approach, Cybersecurity for All (CS4A), to resolve the cybersecurity workforce shortage challenge. CS4A aims to establish new pathways for nontraditional computer and information sciences and lifelong learners to become cybersecurity professionals through continuing education. CS4A addresses the challenge in three steps: identify cybersecurity skills needed to succeed in cybersecurity, create cybersecurity skill stacks to establish pathways to cybersecurity career, and develop flexible and accessible cybersecurity programs for people of all ages. In addition to the current endeavors from government, academia, and industry, CS4A reaches, recruits, and prepares a new talent pool of candidates for cybersecurity workforce and thus help resolve the cybersecurity workforce shortage challenge.

I. Introduction

The cyber threat landscape has changed over in the last 20 years. Cyberattacks are surging and becoming more organized and structured. The technology and tactics used by cyber criminals also become more complicated. The sophistication has outpaced the ability of IT and security professionals to address the threats (Cisco 2015). As a result, data breaches are getting bigger. In a recent data breach in Equifax in 2017, 143 million Americans' sensitive personal information was exposed (FTC 2017). Cybersecurity is a national priority (The White House 2017). However, finding qualified people to help drive successful cybersecurity programs has become a nontrivial task. Cybersecurity skills shortage has become a top challenge for organizations in the world (Suby & Dickson 2015). The 2017 Global Information Workforce Study estimates that the cybersecurity workforce gap will reach 1.8 million by 2022 (Center for Cyber Safety and Education 2017). While government, academia, and industry have worked together to address the cybersecurity skills shortage, it is apparent that more efforts are needed to fill the gap as the data reveals that the cybersecurity skills gap is getting worse (Oltsik 2017).

This paper propose a new approach, Cybersecurity for All (CS4A), to resolve the cybersecurity workforce shortage. An overview of the approach is shown in Figure 1. CS4A aims to establish new pathways for nontraditional computer and information sciences and lifelong learners to become cybersecurity professionals through continuing education.

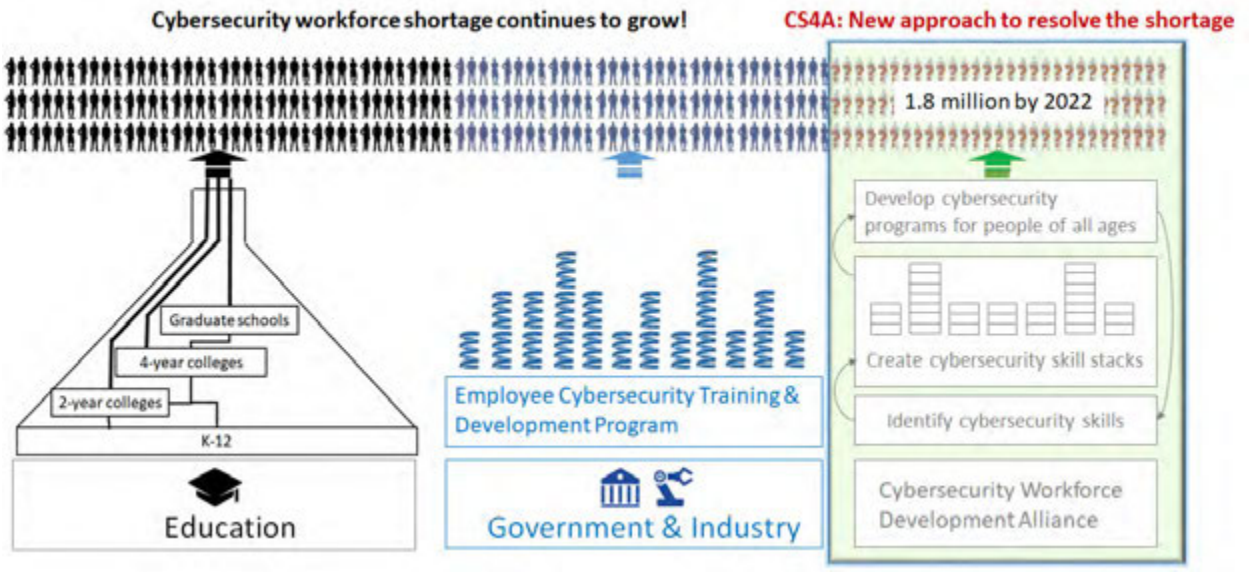


Figure 1. CS4A Overview

II. CS4A: A New Approach for Cybersecurity Workforce Development

A. CS4A Overview

Many initiatives have been put in place to develop cybersecurity workforce. Higher education are adapting curriculums to support cybersecurity program needs. Colleges are taking actions to partner with K-12 and post-secondary schools to engage more students in cybersecurity education. Extra efforts are also being made to attract minority students (e.g., women students) to cybersecurity (A Frost & Sullivan White Paper 2017). In private sectors, many companies and organizations have developed their own on-the-job training programs to train employees to meet their needs in cybersecurity. These endeavors are clearly important and will continue to help build cybersecurity workforce. However, they are far more than enough (Oltsik 2017).

In addition to the traditional academic programs and on-the-job training, the paper proposes a new approach, Cybersecurity for All (CS4A), for cybersecurity workforce development. CS4A targets to a new pool of candidates who are nontraditional computer and information sciences

and lifelong learners. These learners will be most likely declined from any academic cybersecurity programs due to lack of required background. Their daily jobs typically do not involve any cybersecurity duties and will not be able to participate in any on-the-job cybersecurity training. However, they would like to develop their cybersecurity skills through continuing education and prepare them for cybersecurity career in the future. CS4A aims to help this new pool of candidates and help them develop the desired cybersecurity skills. CS4A achieves the goal in three steps: i) identify cybersecurity skills needed to succeed in cybersecurity, create cybersecurity skill stacks to establish pathways to cybersecurity career, and develop flexible and accessible cybersecurity programs for people of all ages.

B. Identify Cybersecurity Skills

The fast changing and sophisticated attacks indicate that the cybersecurity skills needed to prevent those attacks must also be adapted over time. In addition to the skills taught in computer and information sciences, skills such as data analysis and an understanding of risks are also important. To address the cybersecurity skills shortage, it is important to clearly identify what cybersecurity skills are needed to succeed in cybersecurity. This is an important issue for all parties including government, academia, and industry. The paper proposes to form a Cybersecurity Workforce Development Alliance (CSWDA) to lead the efforts. The Alliance includes companies and organizations from both the public and the private sectors.

C. Create Cybersecurity Skill Stacks

Based on the cybersecurity skills identified, the Alliance will create cybersecurity skill stacks which will establish pathways leading to cybersecurity career. Cyberseek (www.cyberseek.org) divides cybersecurity career into three levels: entry-level, mid-level, and advanced-level. The common cybersecurity feeder roles which lead to cybersecurity career includes networking, software development, system engineering, financial and risk analysis, and security intelligence. The cybersecurity skill stacks will establish new pathways for participants to become one of feeder roles as identified by Cyberseek.

The cybersecurity skill stacks will be based on the cybersecurity skills identified in Section II.B. Each stack specifies prerequisite skills required, skills to be developed, and the career path which it may lead to. The cybersecurity skill stacks could be cascaded together horizontally and

vertically. The stacks cascaded horizontally aim to help participants to extend breadth of skills in cybersecurity. The stacks cascaded vertically aim to help participants to develop cybersecurity skills in depth. The stacks will be modulated and can be grouped together based on needs. Certificates can be created for stacks as incentives to participants.

D. Develop Cybersecurity Programs for People of All Ages

Most of the current endeavors of cybersecurity workforce development programs are closed loop. The academic cybersecurity programs are very competitive and selective. Companies and organizations develop training programs to meet their own needs. These programs are generally not available for public. To resolve the cybersecurity workforce shortage challenge, we need to target to a much larger pool of candidates and prepare them to become cybersecurity professionals. CS4A targets a new pool of candidates which are nontraditional computer and information science and lifelong learners. New programs will be developed based on the cybersecurity skill stacks. These programs will be accessible to these learners and also flexible for participants. These new programs may include online programs, vocational schools, certificate programs, etc. The new programs can be sustained with the support from government agencies, academia, and industry.

III. Summary

This paper proposes a new approach, CS4A, to resolve the cybersecurity workforce shortage challenge. Unlike the academic cybersecurity programs and the on-the-job training, CS4A targets to a new pool of talent candidates which are nontraditional computer and information sciences and lifelong learners. CS4A creates new pathways for these leaners to become cybersecurity professionals and thus help resolve the cybersecurity workforce shortage challenge. CS4A can also be used as training programs for students in colleges and continuous training programs for cyber professionals.

References

A Frost & Sullivan White Paper, 2017. *The 2017 Global Information Security Workforce Study : Women in Cybersecurity*, Available at: https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf.

Center for Cyber Safety and Education, 2017. The 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk. *Frost & Sullivan in partnership with Booz Allen Hamilton for ISC2*.

Cisco, 2015. *The Internet of Things : Reduce Security Risks with Automated Policies*, Available at: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/security-risks.pdf.

FTC, 2017. The Equifax Data Breach. Available at: https://www.ftc.gov/equifax-data-breach.

Oltsik, J., 2017. The Life and Times of Cybersecurity Professionals: A Cooperative Research Project by ESG and ISSA. , (November), p.9. Available at: http://www.esg-global.com/.

Suby, M. & Dickson, F., 2015. *The 2015 (ISC)2 Global Information Security Workforce Study*, Available at: http://www.csoonline.com/article/2922381/infosec-careers/confronting-the-widening-infosec-skills-gap.html.

The White House, 2017. President Trump Protects America's Cyber Infrastructure.

Dr. Yong Wang is an Associate Professor in the Beacom College of Computer and Cyber Sciences at Dakota State University. He received his B.S. and M.S.E degrees in Computer Science from Wuhan University (China) in 1995 and 1998, respectively. He received his Ph.D. degree in Computer Science from University of Nebraska-Lincoln in 2007. Before he joined DSU in 2012, he had spent 10 years in telecommunication industry as a senior software engineer and a team leader. His research focuses on network security and privacy issues. His current research projects include mobile, cloud, IoT, and big data. He has published 50+ peer-reviewed papers in prestigious journals/conferences. He is a co-author of three books. He also severs as Technical Program Committee (TPC) members and reviewers for many international conferences in Computer Science. Dr. Wang received four awards from National Science Foundation between 2012 and 2017. He is currently leading the NSF CyberTraining project at DSU.

Ideas (1188 words)

This paper considers the following questions (from **https://www.cerias.purdue.edu/site/nace/**):

- What are the most acute cybersecurity labor supply issues the United States will face in the next 5, 10, 15 and 20 years?
- To address these labor supply issues, what new approaches to cybersecurity education are most needed and why?
- How do we get more US citizens—and a more diverse population —into cybersecurity in meaningful ways?
- What are the proper levels of education to address?

As systems and networks in nearly every industry are increasingly leveraging the efficiencies of the internet, from premise-based to cloud solutions, the relevancy of cybersecurity within these industries increases in like manner. Cybersecurity is integrated throughout each sector of modern society – retail, finance, health, cities, suburbs, schools, workplaces. The pervasiveness of cybersecurity places a heavy demand for individuals who can identify, protect, detect, respond, and recover. If significant changes are not made in how cybersecurity education is approached, the most acute labor supply issues, whether 5, 10, 15, or 20 years out, will be in:

1. Security Engineering – designing security into the vast amount of "things" that will connect to the Internet, especially things that have physical and life/death ramifications if compromised; and
2. Diversity within Machine Learning and Artificial Intelligence – the data used to train machines, and the personnel involved in creating the algorithms for machines and AI, must be accurate, and representative of the population served by the machines, respectively. Otherwise, we will have the same bias in "robots" as we have in human beings, except without the potential counterbalancing aspect of human compassion, or change of heart.

The labor supply issue is an issue of numbers, specifically the number of available, appropriately trained, experienced, and trusted professionals. There are ample United States citizens to address the U.S. cybersecurity shortage, but underrepresented populations must be engaged, starting at

early ages, to address these gaps. There are several barriers that inhibit currently underrepresented populations from becoming successful cybersecurity professionals. Primary inhibitors include:

1. Lack of awareness (e.g. no role models who look like the students, or otherwise, within their everyday environments, and few role models who look like them in mainstream media who, even fictitiously, are in the cybersecurity field);
2. Lack of access (e.g. no computers at home, antiquated or non-existent computers at school, limited transportation to camps or other facilities);
3. Lack of basic needs (refer to Maslow's hierarchy of needs) such that self-actualization in a specific career such as cybersecurity, is fleeting, and quite difficult to obtain;
4. Lack of academic support (e.g. overcrowded classrooms, single parent homes or parents with multiple jobs and limited education that can help with understanding cybersecurity); and
5. Institutionalized discrimination (e.g. the current elementary to prison pipeline, disproportionately, and adversely, impacts minority students).

Exposure to cybersecurity related careers must happen as early as elementary school to plant the seeds of possibility for students. Exposure to these careers must come in the form of classroom learning, after school enrichment, and mentorship, with proportionate representation from role models who look like the students. The students must be able to see themselves – black boys seeing black men, Hispanic girls seeing Hispanic women – in their instructors, in their tutors, and in their mentors. Employers with strong diversity programs can partner with schools, and include mentorship of students as a formal part of employee career development and performance evaluation. Mentorship can be done in person, or accomplished via an online means to expand the reach of each mentor, and better scale the number of students the mentor can effectively impact.

Schools with stretched resources and budgets can also partner with companies to establish a technology endowment program so that technology, while still largely current, can shift from a company to a partnering school. In this way, students have access to learn in a hands-on way, using relevant technology.

The lack of basic needs and academic support are not easy problems to solve, and certainly require the participation of family, community organizations, government, and industry. The approaches taken to meet basic needs and provide ample academic support must be sustainable, and based in an economic model that educates and empowers, not only the students, but their family and social network.

Cybersecurity is a field that requires trusted individuals, and students must learn early on that antisocial and criminal activities can drastically impair their ability to participate in such promising fields as cybersecurity. This is another reason why exposure to cybersecurity education and careers should start as early as elementary school, so that children can start making decisions consistent with a field they may find interesting.

Publicly traded privatized prison companies use student test scores, starting from as early as third grade, and other student home factors to project future prison populations. Schools are using policing in a way that criminalizes student behavior without addressing root causes. If algorithms and school policies can be created and used to project and yield a negative outcome and situation for students, then the same algorithms and policies can be turned on their head and used as a means to identify populations to target for technical skills training and education that lead to lawful, promising careers in fields such as cybersecurity. The pipeline to prison must be disrupted to redirect the talent to a cybersecurity pipeline instead. Some of our country's most brilliant minds are put behind bars at early ages, and perpetually trapped in the justice system, but these brilliant minds can be tapped to address instead a dire need in our country.

Cybersecurity education should be approached in a way that demonstrates how cybersecurity is present in the everyday lives and interactions of students. In this way, learners are able to make a connection between the broad term of "cybersecurity" and their everyday lives. Further, to make cybersecurity more accessible to broader populations, cybersecurity education should be approached by making analogies to long standing and understood systems, environments, and principles. As an example, computer networks can be compared to a home; intrusion detection systems can be compared to home alarm systems; computer viruses can be understood through comparison to human viruses. While cyberspace is a "new" domain, there are multiple long existing domains that can be used as a basis of comparison and learning for cybersecurity. This approach to education is already happening with such disciplines as biomimicry, where biological systems are used to drive the design and function of computer networks.

This "teach by analogy" approach to education would include the following broad steps:

1. Identify the industries, systems, and other aspects of the target learner population's everyday environment (e.g. inner city, reservation, rural);
2. Leverage the target learner population's understanding of their everyday environment to explain cybersecurity concepts;
3. Engage learners in opportunities to think through solutions that apply to their everyday environment, and then challenge them to extend the solutions to convey the analogous application in cyberspace;
4. Provide access to the tools necessary for the learners to prototype and demonstrate their cybersecurity solutions.

By approaching education in this way, learners are trained to see cybersecurity as an integrated, multidisciplinary field with broad applications in everyday life.

Author Biography (158 words)

Tina C. Williams-Koroma – Esq., CISSP, PMP, is founder and President of TCecure LLC, a cybersecurity services company based in Maryland. Tina has 15+ years of experience working in the cybersecurity field, providing services to public sector and commercial clients. She possesses a B.S. in Computer Science from the University of Maryland Baltimore County (UMBC), a M.S. in Management from Rensselaer, and a J.D. from the University of Maryland Francis King Carey School of Law. She is a member of the Maryland Bar and the CyberMaryland, NICE365 Industry Advisory, and UMBC Research Park Boards of Directors, and is an Adjunct Instructor at UMBC for the Masters of Professional Studies in Cybersecurity. Further, through a TCecure contract with the University System of Maryland, Tina is the Cybersecurity Academic Innovation Officer for the National Cybersecurity Federally Funded Research and Development Center (FFRDC), responsible for integrating academic research and resources into the National Cybersecurity Center of Excellence (NCCoE).

CybSec Champions Fellowship

Purpose/need: There has been great attention on the need to fill the cyber security work force. With the focus largely on college students and veterans re-entry into the work force, recently, the focus has been shifted to high school age and under. Providing programs targeted to this age group has started with competitions such as CyberPatriot and CTFs and programs to support specific groups such as girls through avenues like Aspirations in Computing and Girls Who Code, people are understanding the need to start training and supporting the younger generation. Without planting the seed at a younger age, there will continue to be a shortage in supply for the cyber security workforce. Without having young people grow up with the vocabulary of security in this technology driven world, there will never be a shift in culture that embraces security as an integral part of ensuring the balance of the cost of technology.

I propose the missing piece in the work that is being done in the investment in the people investing in the development of these young people. "Champions" that have been fighting to ensure that young people are being exposed to opportunities will not only better the young person's future, but will also contribute to the betterment of the world. Champions might be school teachers or girl scout leaders or after school providers, but they all share similar traits: be passionate about their vision of what the world should be like and be willing to put in the work to see it happen (evidenced by the countless "volunteer" hours of work they dedicate), be passionate about the hope they place in young people, have an understanding about the system we live in (economic mobility only exists if young people are trained in an area that they will have an opportunity to find work), and look at the world in the broader sense (in order for us to be "safe," we must be the ones defending). Like super heroes, these champions view their role in society as agents of change with a code that they live their lives by. This population of people can often be found coaching cyber competition teams, starting a chapter of a local Girls Who Code group or volunteering to be a Girl Scout leader. There are few resources widely available for these champions to develop and be even more supportive to the young people they work with. However, champions have learned to be resourceful and forage along the way and find what they need along the way to be the best champion they can be for the young people they work with. There needs to be a system (program) in place to support the people supporting the young people so that this pool of talent can even make it to the next level, which could be college or directly to the work force.

Roles/players:

Champion: Teacher, Community volunteer, after school provider or anyone else not in a traditional role that is supported but would benefit from professional development/mentoring specific to the cyber security field.

Mentor: A person at an institution of higher learning or even an industry partner dedicated to being part of the pipeline of ensuring the growth of the pool of applicants in the security field. Willing to invest time and resources to be a part of a team of adults supporting the young people the Champions work with.

Program Manager: Someone who is overseeing the implementation of the program and ensuring documentation and paperwork is being handled accordingly.

Program overview: Cohort of Champions will be chosen and matched with Mentors in their state. Reason, so that they are able to create a local support network. On average, about 72 percent of high school students stay in state when attending college (www.statisticbrain.com/percentage-of-out-of state-students-at-public-universities). This will give the Mentor who works an edge in encouraging these students to attend the school he/she represents. He/she will have developed a relationship and support the young person in his/her transition, a continuation of support through the "pipeline." For an Industry Mentor, his/her role can be and not limited to helping plant the seed of the end goal, of finding work and supporting the steps necessary to get there. Benefit for Industry partners (mentors) is a pool of young people they would be able to recruit to work for the Industry partner's company, either right out of high school or out of college. The perfect triad would be Industry, Higher Ed, and the Champion. Benefits for the Higher Ed Mentor would be to link his/her students with Industry partner as well. Champions would benefit from the resources provided by his/her mentors to bring back to students. From curriculum to pool of people to bring in for career awareness opportunities, everyone would benefit.

Program Components:

- Champion would meet with Mentor(s) at least once a month to check in on needs and opportunities. This could be done virtually or in person. Ideal situation would be to meet, then to also meet with students participating.
- Champion would have an opportunity (funding) to attend at least 1 conference for development and networking opportunities.
- Champion will work with Mentor(s) to develop a project/research to further the development of cyber education. Examples, but not limited to gamifying cyber security, curriculum for high school or middle school aged students, events to target growing interest in cyber security, especially in underserved areas. Project/research would be presented at an event such as CISSE and/or locally at an ISSA event.
- Champion and possibly Mentors will receive a stipend for their commitment to the Fellowship.
- Champion will commit to minimum of 1 year. Possible to grow Fellowship to 2 years if he/she returns as a Mentor to next cohort.

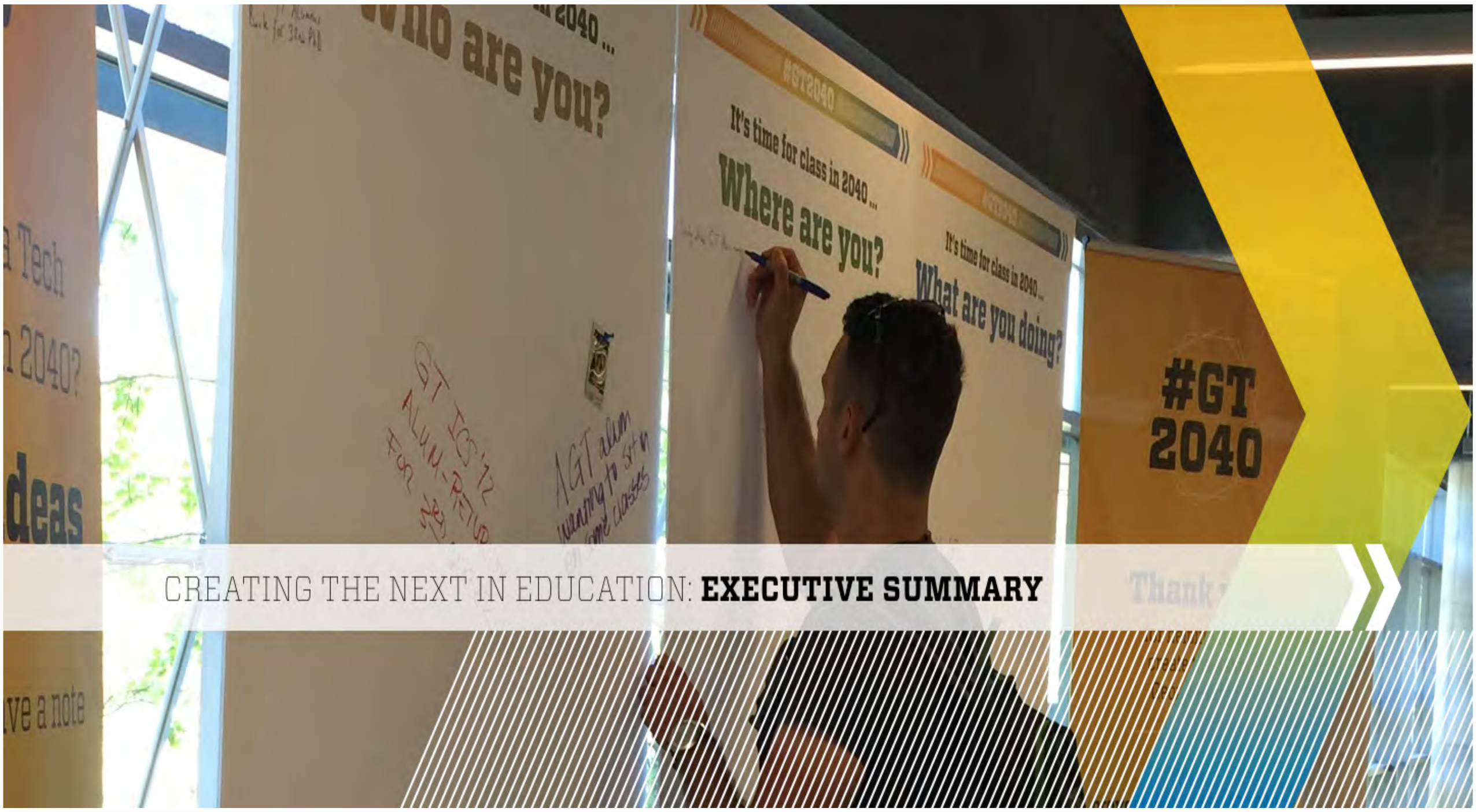
Qualifications of Champions/Who should apply?

- Majority percentage of applicants should be people with a proven track record of their commitment to cyber security education to middle and high school students.
- Small percentage of Fellows should/can be newbies who are looking for help getting started.
- Works directly with middle or high school youth (preference given to those working with underserved communities)
- Benefit from a mentorship to grow the work that they are currently doing

Outcomes:

- Project or research that is developed by Champion (deliverable).
- Still not sure how to measure student success—possibly the number of students served by the Champion that go into Cyber Security as a major/minor or go into Industry out of high school.
- TBD

There are still a lot of questions and details to work out, but I believe this is a strong start to the discussion of the need to include and support the role of the Champion who sometimes do not fall into traditional titles and therefore is not supported to continue the work that they do. Access, opportunity and support are the key factors that I feel are lacking for Champions currently. Many Champions have managed to navigate and find a way despite the lack of real direction and support, but I propose that there is a way to provide that support. I believe a program such as the CybSec Champion Fellowship could be valuable as one approach to address the need to educate and help the direction of cyber security.



Executive Summary

This moment is ripe for change in higher education. Scores of technology entrepreneurs, foundations, and policymakers are already trying to shape what the future looks like for both learners and institutions. The message for colleges and universities is clear: they can either sit idly by or join in to design their own destiny. As a selective public institution with a history of educational innovation, the Georgia Institute of Technology sits squarely in the middle of the forces shaping higher education. It is uniquely positioned to model what the university of the future might look like.

This report of the **Georgia Tech Commission on Creating the Next in Education (CNE)** is an effort to draw with broad strokes the nature of education that defines the technological research university of the year 2040 and beyond. The Commission was formed because many within the institution are convinced that by the second half of this century Georgia Tech will be different from the university that matured and prospered in the nineteenth and twentieth centuries. Georgia Tech's mission seems to demand that the Institute examine the choices that lie ahead and make plans for a future that, however uncertain, is bound to present opportunities and challenges that cannot be understood as incremental changes in the status quo.

Drivers of Change

In a prior report titled *Discovering the Drivers of Change in Higher Education* (Georgia Tech 2016), the Commission outlined the forces likely to affect Georgia Tech, including a new and accelerating revolution characterized by technology-driven disruptive change throughout society, shifting public attitudes about the role of public universities, and demographic trends that challenge long-held assumptions about who will benefit from a college education. Upon publication of that report, the Commission engaged in a broad search for ideas about how best to anticipate the kinds of changes that are certainly in store for Georgia Tech and to synthesize a roadmap for the future.

The Georgia Tech Commitment

The overarching recommendation of the Commission is an ambitious proposal called the **Georgia Tech Commitment to a Lifetime Education**. It is a concept unlike anything that exists today—a future for college not conceived solely just as a physical place one enters at a particular age and exits when a degree is completed but rather as a platform for an increasingly diverse population of learners.

By the year 2040, Georgia Tech learners will be more ethnically and socioeconomically diverse. Some will be much younger than traditional undergraduates; others will be much older. Neither group will resemble the traditional, residential college student in terms of their expectations or demands. Their numbers may far exceed the current residential enrollment. The Georgia Tech Commitment is a promise to these new learners to provide the rigorous, high-quality experience that has defined a Georgia Tech education for more than 130 years but to do it in a way that is individually personalized and sustainable for a lifetime. This commitment is a promise to invest in the success of all Georgia Tech students.

For the Georgia Tech Commitment to become a reality, the Institute must redefine its fundamental approach to educational delivery with four key actions: eliminate artificial barriers between college and pre-college schooling, invent flexible educational pathways and credentials that recognize continual learning, reinvent the physical presence of a university for a worldwide population of learners, and provide advising and coaching networks that serve the lifetime needs of Georgia Tech learners of all ages.

Innovation is required for each of these steps to be successful. An integral part of delivering on the promise of the Georgia Tech Commitment is a set of initiatives that are aimed at closing knowledge gaps, prototyping new products and services, and building technological infrastructure that enables this broad expansion of Georgia Tech's mission.

These initiatives are conceived as research programs that will be launched upon completion of the Commission's work. They will be planned and managed by an expanded ecosystem for educational innovation.

The Initiatives

The Commission identified five initiatives to better understand the challenges standing in the way of achieving the vision of the Georgia Tech Commitment and to create tools, invent methods, and collect data that will be required to make progress. Included in these initiatives are immediate actions and longer-term projects that will require both invention and sustained research. These initiatives address problems that the Commission believes are on every critical path to the Georgia Tech Commitment and many other conceivable futures as well.

Initiative 1: Whole-Person Education

Georgia Tech graduates have a reputation for strong technical skills and initiative, but, increasingly, other skills are needed for success in the twenty-first century workplace, including cognitive skills, such as problem solving and creativity; interpersonal skills, such as communications and leadership; and intrapersonal skills, such as adaptability and discipline. The Commission found that virtually all employers consider these skills to be a distinguishing characteristic for long-term success. Employers look to leading colleges and universities to provide graduates who have not only deep disciplinary knowledge but also these additional skills.

This initiative consists of four interrelated projects that address important aspects of delivering whole-person education to Georgia Tech learners:

1. Experiential learning that embeds the learning experience in authentic, relevant contexts.
2. Globalization at home to develop a culture in which critical thinking and collaboration can be taught in the context of a multicultural world.
3. Professional development of graduate students that fuses whole-person education with the more research-oriented training typical of graduate education.
4. A new whole-person curriculum that emphasizes interpersonal and intrapersonal dimensions of education in addition to cognitive dimensions.

Initiative 2: New Products and Services

To meet the demands of evolving job markets and the desires of a widely disparate population of future learners, the Georgia Tech Commitment calls for flexible learning experiences and continual learning opportunities. New products will need to be created that afford future learners the ability to customize their educational experiences. Development of these new educational products and services will be enabled by four projects that address both near-term and long-term problems:

1. Microcredentials to create more efficient packages of experience and achievement.
2. A matrix of minimester classes that will allow students to replace monolithic three-credit-hour classes with more granular and flexible modules.
3. A new credit-for- accomplishment unit measured by demonstrated competencies and skills.
4. A new decentralized transcript based on blockchain technology that allows students to combine evidence of learning and achievements into credentials that are relevant to potential employers.

Initiative 3: Advising for a New Era

Advising for a new era is a challenge to the traditional fragmented approaches to advising. The Commission recommends a robust learner data backbone as well as artificial intelligence assistants that integrate prescriptive, intrusive, and developmental advising services to personalize them and provide a new advising experience, at scale, to learners of all types. Three projects are key to launching this initiative:

1. Personalized advising for effective and scalable advising services tailored to the needs and prospects of individuals at all stages of life.
2. Technology-enhanced advising to deliver new ways for supporting personalization at scale.
3. Personal Boards of Directors to create professional networks for Georgia Tech learners.

Initiative 4: Artificial Intelligence (AI) and Personalization

Georgia Tech has led in the development of AI-based personalization systems. The "Jill Watson" experiment used the IBM Watson system as the basis for an artificially intelligent teaching assistant and was widely hailed as a breakthrough in both AI and educational technology. The opportunity now exists to augment "Jill's" skills to handle other tasks that are associated with personalized learning. A multifunction virtual tutor can be deployed to advisors, coaches, and even mentors located at distributed Georgia Tech locations around the world. Three projects are envisioned as part of this initiative:

1. Pilots for mastery-learning and adaptive-learning platforms that can put the kind of technology that will allow customized delivery of material into the hands of learners within two years.
2. Personalized and multifunctional tutors to take advantage of advances in AI to push the envelope in personalized learning.
3. Human-centered AI to support the development of interactive AI agents whose interactions with humans are informed by cognitive models and contexts.

Initiative 5: A Distributed Worldwide Presence

The idea of a physical campus—a designed space for students, teachers, and educational programs—has been a mainstay of the college learning experience for a thousand years. The physical campus is, however, a fragile model. A campus has the advantage of making educational facilities broadly available, but it does not necessarily match services to regional needs.

The Georgia Tech Commitment values the personal presence of instructors and advisors in the educational experience but recognizes that problems of scale and expense will limit the number and kind of such deployments. It is always an option to provide remote or online facilities to connect new students to a central campus, but Georgia Tech's experience with affordable online master's degrees convinced the Commission that there are better ways to create a real presence as part of the Georgia Tech learning experience. The following projects will enable experimentation with new modes of student interaction:

1. *The Georgia Tech atrium*™, a concept that recreates in other locations the scalable gathering places and portals to educational services that have become ubiquitous on Georgia Tech's central campus. These spaces can be located near clusters of Georgia Tech learners in co-working spaces, corporate offices, or even retail malls. Each atrium can be programmed to suit the needs of local learners and can provide cost-effective, high-quality educational experiences to Georgia Tech students and others by matching personnel, expertise, and facilities to the needs of the communities served.
2. *A Living Library for Learning (L3)* that expands an already successful network of Human Libraries to a broad range of educational contexts. Through an L3 portal, Georgia Tech will be able to provide personal, on-demand access to individuals who have first-hand experiences to relate to classes or individual learners. The Human Library vision of "loaning people, not books" has great appeal for technological universities.

The Culture of a Deliberately Innovative Organization

The five initiatives represent radical departures from usual ways of delivering rigorous university-level learning experiences. The pace of innovation required to achieve their goals is daunting. Recognizing the often-slow pace of change in higher education, the Commission envisions a long-term process for instilling in the culture of Georgia Tech the ability to innovate in a more predictable and timely way, moving to becoming a more deliberately innovative university.

The Georgia Tech Lifetime Commitment and the initiatives proposed to achieve it are bold, and they need to be supported by an underlying culture of educational innovation that is both robust and agile so that it can adapt to disruptive forces and a rapidly increasing rate of change in technology and society. Georgia Tech's current culture has produced internationally recognized innovations in education that have had great impact, but the Commission feels there are still cultural shifts that would improve the university's capacity for continuing innovations. By making innovation processes the subject of study and applying research-based methodologies, the Commission believes that Georgia Tech can become a more deliberately innovative organization.

A systems approach would allow the examination of innovation processes in interacting groups of people and organizations, and it would support taking deliberate actions to improve desired outcomes over time. The Commission envisions five steps that are necessary to launch the Institute onto this pathway.

Merging Two Successful Cultures

Georgia Tech's capacity for educational innovation has grown dramatically over the past decade, but to a large extent, successful innovation in education is still not systematic. Inventions germinate and successfully change the way education is delivered, but success or failure seems to depend as much on luck or circumstance as on merit or need. The Commission imagines a merger of two existing, successful cultures for innovation: a grassroots culture and an institutional culture. Each culture is individually effective, but aligning the two will create a more agile and sustainable environment for innovation.

A Systems Approach to Becoming Deliberately Innovative

A systems approach to creating a deliberately innovative organization improves on current successful models of innovation. The Commission recommends long-term steps to immerse educational innovation practices in the kinds of cultures that are known to enhance innovation at the enterprise and organizational levels, shifting academic structure and processes when necessary to better align with those known to promote innovation.

Enhancing the Innovation Ecosystem

The Commission examined ways that the current educational innovation ecosystem might evolve into a broader, more coordinated entity, with expanded scope and range. A great advantage enjoyed by Georgia Tech is its vibrant research environment. The Commission recommends fusing the values and mindsets of research and education communities at all levels of university operation and governance.

Bridging Organizational Silos

Organizational silos are policies, procedures, or cultural limits that inhibit people of different groups from free interaction. An academic example is disciplinary silos. New organizational and financial models will help to bridge these silos.

Motivating Individuals in the Innovation Process

The Commission recommends policies that acknowledge, reward, and incentivize faculty and department leaders to pursue educational innovation. Everyone at Georgia Tech should be immersed in a culture of educational innovation. Every investment decision should be steeped in it. The Commission endorses total immersion, but it will take time to create conditions that connect the individual goals and aspirations of Georgia Tech's faculty and students with the goals of the Georgia Tech Commitment. It is an opportunity for individuals to grow by leveraging what they know while being honest about what they do not know and by taking risks while thinking through worst-case scenarios.

What's Next?

Demographic and economic forecasts gathered during the six-month discovery phase that kicked off the Commission's work paint a clear picture: higher education institutions of all kinds are facing a far different future compared to the world to which they have become accustomed. In many ways, the current challenges facing

higher education are similar to the ones that confronted Georgia Tech at its founding. Today's challenges, like those of the mid-nineteenth century, are the consequence of rapidly expanding knowledge, industrial revolution, and immense change in the world economy.

In the previous era, colleges and universities and their leaders approached those changes with great optimism and a feeling that change was an opportunity for growth. The Commission believes that spirit can be rekindled today. A group of universities will need to lead higher education through the changes promised in this next decade and beyond. Georgia Tech is determined to be in this group by expanding its mission to include the Georgia Tech Commitment to a Lifetime Education.

The roadmap presented here is a result of looking up and out to grasp the bigger picture of higher education and its future. We imagine a future where artificial barriers that have existed in education disappear and the role that people and technology play in guiding students in their lifelong educational journeys is better understood. In such a future, new educational products will be needed, and, as simple skill acquisition becomes easier to achieve, the whole-person education needed to prepare individuals for new workplaces will become an essential part of higher education. Finally, the success of all the projects described in this report is predicated on an immersive culture that fosters deliberate innovation.

Access to higher education and scholarly research has long been the lever universities have pulled to promote their prestige. In higher education it is difficult, if not impossible, to stray far from the pack and think differently about how to engage new generations of students and how to provide them with the most immersive educational environment, all while being on the cutting edge of the next discoveries in the world. But the changing needs of both the global economy and higher education demand that universities like Georgia Tech move in a new direction to remain relevant in an increasingly automated and diverse world.

Timeline of Commission Activities

View Full Size

« Previous Page: Report Home

Next Page: Introduction »

Cybersecurity Ethics Education: On "Future-Proofing" the Education We Provide

In this idea paper, I propose a kind of ethics education for cybersecurity that I believe is needed if we are to have any hope of "future-proofing" the education we provide. Cybersecurity education equips students to take profound action in the world and at the same time positions them to operate in a space in which the rules are often ill-defined. The field of cybersecurity is far from establishing codified standards of ethics and the few laws we do have in this area lag woefully behind the speed of technological innovation. We must recognize that we are educating the decision makers of tomorrow who will play a significant role in shaping the future of society. Amidst the rush to prepare a generation of cybersecurity professionals, this requires that we develop long term educational innovations that can prepare tomorrow's thought leaders for the unknown and uncertain futures before them.

Although it is encouraging that the NICE Cybersecurity Workforce Framework and the CAE Knowledge Units, two of the major curricular guidelines for cybersecurity, address ethics in cybersecurity, they both rely on a rule- and compliance-based approach to ethics education. The NICE Framework includes knowledge of ethical hacking principles and techniques as well as knowledge of national and international laws, regulation, policies and ethics as they relate to cybersecurity.[1] Similarly, included among the CAE Core Knowledge Units is: Policy, Legal, Ethics and Compliance. This knowledge unit intends "to provide students with an understanding of information assurance in context of the rules and guidelines that control them," by having students list and describe applicable laws and policies, which includes responsibilities for handling vulnerabilities.[2]

While knowledge of relevant laws and policies are an important place to begin, I believe that a rule- and compliance-based approach to ethics education is insufficient for cybersecurity. I briefly offer two reasons for this, here. First, because our laws cannot keep up with the speed of technological innovation. A preeminent example supporting this claim is the chief law we have for regulating cyberspace, the 1986 Computer Fraud and Abuse Act (CFAA), which, according to Josephinne Wolff's recent analysis of five cases, struggles to

[1] Newhouse, William, Stephanie Keith, Benjamin Scribner, and Greg Witte. "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework." *NIST Special Publication* 800 (2017): 181, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

[2] CAE Community, "Policy, Legal, Ethics and Compliance," Core Knowledge Units (2018). https://www.caecommunity.org/resources/ku-cards/ku/policy-legal-ethics-and-compliance.

> regulate a space where, fundamentally, some of the activities we want to encourage among the good guys—finding new vulnerabilities in computer systems, testing the security of software and devices—are largely indistinguishable from the activities that we want to discourage when undertaken by the bad guys.[3]

We are preparing students to operate in a realm that is not yet well contained by laws, standards, and norms. We need to recognize this by preparing students to not only have knowledge of yesterday's rules and laws, but to also be able to envision and establish the norms, rules, and policies of tomorrow.

Second, I draw on the educational philosophy of John Dewey in claiming that an ethics education of direct instruction in following the rules only amounts to something "in the degree to which pupils happen to be already animated by a sympathetic and dignified regard for the sentiments of others. Without such a regard, it has no more influence on character than information about the mountains of Asia."[4] A student's own inclinations and prior beliefs play a significant role in determining their ethical conduct. Cybersecurity ethics education must recognize this and find innovative ways to draw upon students' own ethical inclinations. Dewey continues, maintaining that within a democratic society, to attempt to get reliable results through an ethics education of direct instruction is "to rely upon sentimental magic."[5] There is an irony here in that ostensively, we are endeavoring to develop a cybersecurity workforce in order to uphold our democratic society. Yet, in the case of cybersecurity ethics education, I suggest that we not only need to educate *for* democracy, but *through* it as well.

I conclude by proposing an alternative approach to cybersecurity ethics education that involves creating intentional space for engaging in a cumulative and ongoing process of ethical inquiry. In addition to imparting knowledge of relevant laws and ethical principles and practices, there is a need to cultivate wide-ranging capacities, skills, and dispositions that will enable cybersecurity professionals to utilize, reflect upon, and revise this knowledge-base throughout their careers. The aim of this alternative approach is to foster a kind of ethical culture that can endure in the face of uncertainty and ever-emerging potentialities.

---

[3] Wolff, Josephine Wolff, "The Hacking Law that Can't Hack It," *Slate* (2016), http://www.slate.com/articles/technology/future_tense/2016/09/the_computer_fraud_and_abuse_act_turns_30_years_old.html.

[4] John Dewey, *Democracy and Education*, New York: The Free Press (1916), 354.

[5] Ibid.

Jane Blanken-Webb is a Postdoctoral Research Associate at the Information Trust Institute at the University of Illinois at Urbana-Champaign, where she is taking the lead as co-principal investigator on a grant funded initiative, Ethical Thinking in Cyber Space (EThiCS), supported by the National Security Agency. The main aim of this grant is to develop and teach a cybersecurity ethics curriculum, which was piloted during the Spring semester of 2018. She holds a PhD specializing in Philosophy of Education from the University of Illinois at Urbana-Champaign and her work has been published widely in the field of education. In addition to extensive teaching experience at the university level, she has four years of experience teaching in K-12 environments. Jane and has been working in cybersecurity education since the Fall of 2016 and is closely involved with the Illinois Cyber Security Scholars Program, an NSF funded Scholarship for Service program.

SEVEN OVERLAPPING THESES ON CYBER-SECURITY EDUCATION

Scott Borg
Director and Chief Economist
U.S. Cyber Consequences Unit
scott.borg@usccu.us

The majority of the leading figures in real-world cyber security did not become the acknowledged masters of the field *despite* their unconventional and diverse academic backgrounds; they became the acknowledged masters *because* of their unconventional and diverse backgrounds. Entering the field of cyber security before there were regular university programs or even courses in the subject was actually an advantage. The current formalization of cyber-security training is in danger of actively *preventing* people from developing many of the skills and abilities that the field most needs. What's more, many of the proposals for improving cyber-security education would only make things worse.

The following seven theses are all essentially an elaboration of this point. They are based on many years of intensive, practical experience in cyber security, including in-depth, on-site investigations of nearly all the critical infrastructure industries. There wasn't room to describe the relevant experiences in this short paper. Most people with extensive practical experience in cyber security, however, will be able to think of many anecdotes that would support these seven theses.

Obviously, we need formal cyber-security training. We need far more practioners than could ever be produced or find their way into the field without regular academic programs. But we need to be sure that those programs are preserving at least some of the features that made many of the pioneering people in the field so adept and so innovative. We need to be sure we

are preparing people not just for entry level jobs, but for future leadership roles. We especially need to be sure that we are not doing things in our training programs that put our graduates at a disadvantage when it come to dealing with highly creative adversaries.

Thesis One: An over-emphasis on STEM training is often making students *less* equipped to do cyber security well. The subject matter of natural science, engineering, and math, can be predicted by extrapolating from past cases. As Einstein famously said, nature is subtle, but it is not malicious. The uncertainties in natural science can usually be modeled by normal distributions. The subject matter of cyber security is not like that. Cyber attacks, their practical consequences, and the ways they can be foiled cannot be predicted by extrapolating from past cases. Cyber-security practitioners regularly need to deal with phenomena that are not just subtle, but malicious and cunningly so. The uncertainties in the field can hardly ever be accurately modeled as normal distributions. The often dazzling creativity of cyber attackers needs to be met with equally dazzling creativity on the part of defenders. When systems are under attack, defensive actions often need to be taken based on an intuitive assessment of what is going on, with no time for a comprehensive, carefully reasoned analysis, testing, or verification. Yet at the same time, the field is so open-ended, there is no objective way to put a limit on the facts that need to be taken into account. The whole mindset of natural science, engineering, and math is therefore profoundly wrong for doing cyber security.

Thesis Two: The information assurance triad of availability, confidentiality, and integrity, which still dominates cyber-security education, is obsolete as the goal for cyber security. This is because these categories describe features of information systems and cause defenders to focus on their own technology, rather than on potential attackers. The goal of cyber security should be to reduce risk, defined as annualized expected loss. The way to do this is usually to increase attacker costs. This means that the focus, even at a very basic, practical level, should be on stopping the things that attackers need to do in order to make their attacks pay off. Cyber security practitioners, guided by the information assurance triad, can rarely describe with any accuracy more than one or two components of what they are trying to

prevent. Many of the most notorious cyber-security failures over the last several years can be traced to this failure in understanding.

Thesis Three: The *majority* of the topics cyber-security professionals most need to master in order to assess and reduce cyber risk are *not* covered in the curricula of most university cyber-security programs. This is partly because they are not included in the $(ISC)^2$ Common Body of Knowledge used for the CISSP exam, the NIST Cybersecurity Framework, or the other documents regarded by academics as defining the field. As a result, most cyber-security education focuses overwhelmingly on a narrow technical portion of the Vulnerability factor in the cyber-security risk equation. It largely ignores the other two factors in the risk equation: Consequence and Threat. When cyber-security programs pretend to address these other factors, they usually define them in a way that reduces them to aspects of Vulnerability. Despite the fact that economic factors drive almost everything that happens in cyber security, most cyber-security programs omit economics altogether. Even the specializations in cyber-security education are focused the wrong subjects. If cyber security is going to reduce risk, it needs to tailor its practices to the different economic and safety requirements of different industries. Yet cyber-security specializations are rarely organized by industry. Instead, the usual specializations regularly separate issues that, in practice, need to be handled together and by the same person. The NICE Framework, for example, puts many tasks into different work roles and different specialty areas that should never be performed by different people. Meanwhile, this same NICE Framework fails to distinguish between the very different cyber-security requirements of industries as distinct as railways, electronic manufacturing, healthcare, and financial services. At both a basic and an advanced specialist level, expecting cyber-security practitioners to protect industry systems without any genuine understanding of what those systems actually do, technically and economically, is a very bad educational strategy.

Thesis Four: The qualification hurdles designed to make sure that cyber-security professionals cannot get accredited without the types of expertise deemed most essential are effectively *excluding* the kinds of skills and expertise that are *really* most essential. Cyber security does not need practitioners who will faithfully do exactly what they were taught in

school nearly as much as it needs people who can tackle a subject without being told what to do. It does not need people who can remember exactly what they were taught nearly as much as it needs people who can continually re-think things, and who can move across different disciplines so casually that they are barely aware of doing so. Before there were university departments in computer engineering, programmers were typically recruited from language departments, philosophy departments, linguistics departments, and even music departments. The broader liberal arts background associated with those fields of study was often more valuable for their later work than any specific training they received in matters relating to computers.

Thesis Five: The effort to make the study of computers and programming academically respectable, by describing it as a "science," rather than as a field of engineering, and by emphasizing mathematics, especially the mathematics of analog physics, has caused adverse effects on cyber-security education that urgently need to be corrected. Hardly any of the mathematics computer engineering students are required to learn is of any practical use in practical programming, let alone cyber security. This means that the math requirements in computer engineering and cyber-security programs severely limit the available talent pool without delivering any compensating benefits. Worse, treating computer engineering as though it were a science to be pursued for science's sake results in graduates who design programs and systems that are too fragile for the real world. It is as though engineers were being taught to design bridges "for bridge's sake," without ever having to worry about things like traffic, winds, earth tremors, metal fatigue, temperature changes, and future uses. Companies often have to train "computer science" graduates from our best universities for an additional year-and-a-half to two years before they can use them for anything important. Even then, these graduates tend to retain work habits that are not conducive to things like secure programming.

Thesis Six: Where cyber security is concerned, cultural diversity is not a laudable social goal, but a *functional* necessity, and, even though most educational programs for cyber-security education pretend to encourage this diversity, they actually go to great lengths to eliminate it. One of the ways educational programs do this is by assuming that the correct answer to

almost every problem or test question will be same for every student. Real-world cyber security, however, depends on people seeing things differently, especially seeing things other people have missed, not only different ways of accomplishing the same things, but different things that could be accomplished. Cyber-security training should be encouraging and rewarding students who can come up with a *different* answer than anyone else. This is the opposite of current practice.

Thesis Seven: The technical jargon currently used in the profession and in many cyber-security courses is an obstacle to good cyber-security education. This is not primarily because of the barriers it puts between cyber-security professionals and the general public, but because it is riddled with fallacious assumptions, obsolete distinctions, category confusions, and usages inconsistent with better established disciplines. The terms used to describe cyber attacks, for example, do not follow any consistent principle. Some terms refer to propagation mechanisms, some to hiding places, some to activation times, some to attacker goals, some to technical effects, some to business effects, and so on, through at least sixteen principles of classification. The definitions cyber-security authorities, such as NIST, give for basic business and financial terms, such as "asset" and "risk," are often simply wrong. What's more, students tend to learn the technical terms, instead of the underlying concepts, and then get even the technical terms wrong. Despite these problems, most cyber-security programs, instead of making stringent efforts to avoid the jargon, pride themselves on teaching it. This has the further effect of making most cyber-security graduates incapable of defending their budgets when they are talking with senior business executives.

Scott Borg is Director and Chief Economist of the U.S. Cyber Consequences Unit, an independent, nonprofit research institute that investigates the strategic and economic consequences of cyber attacks. He is the leading authority on the economics of cyber security as well as a number of technical topics. He has been the principal proponent of a quantitative, risk-based approach to cyber security for nearly twenty years and is responsible for many of the concepts that are currently used to understand the effects of cyber attacks in business contexts. He is author of The ISA Guidelines for Securing the Electronic Supply Chain, the most comprehensive reference document for protecting electronics manufacturing. Along with John Bumgarner, he is co-author of the new US-CCU Cyber-Security Matrix, a complete survey of genuinely useful cyber defense measures, more than a thousand items long, organized according to the attacker activities they are designed to prevent. His other technical contributions have included pioneering work on the techniques for hiding and finding malware and new methods for analyzing it. Partly because of the way he has been able to employ economic models, his record for anticipating new developments in cyber security since 2002 is probably unequaled. He was able to predict Stuxnet, for example, its exact target, and exactly how it would reach and damage that target, fourteen months before it as found. He has been quoted in most of the world's leading news publications, comments for NBC, CNN, the BBC, NPR and other broadcast media, served on the Commission on Cybersecurity for the 44th Presidency, and has lectured at Harvard, Columbia, Berlin (Freie), and other leading universities. His current research is on the implications of cyber security for international relations.

New Approaches to Cybersecurity Education (NACE) Workshop
Topic: Making Socio-Technical Cybersecurity a Part of Educational Preparation
Chris Bronk and Wm. Arthur Conklin
University of Houston

Summary

While cybersecurity was once a small niche area, primarily, but not entirely contained in computer science and engineering, it is increasingly viewed as a significant societal problem. Getting "hacked" is a relatable experience to millions of Americans in personal or professional venues. But finding remedy or protection is far harder than being compromised by cyberattack. For this reason, we propose effort on connecting to disciplines in developing fundamental learning injects for cybersecurity that align with other forms of professional responsibility and ethics.

The Problem: Cybersecurity Outside the Cybersecurity "Priesthood"

Cybersecurity has become a fundamental component of the socio-technical environment where an enormous amount of work takes place. Professional activity in all manner of endeavor and enterprise is dependent upon a technological infrastructure that remains inherently insecure. Thus far, the primary response to our societal cybersecurity problem has been cybersecurity chiefly as a technical design objective; something to be engineered into a tool, a product, or a process. This focus on "build to deploy" efforts has resolved some issues but falls short of comprehensive remedy. Effective cybersecurity over the long-term requires greater breadth and wider penetration of cybersecurity behaviors across the entire range of activities enabled by information and computing technologies.

While we work to expand the professional cybersecurity workforce, there is an enormous unresolved question regarding our current efforts: *How do we integrate cybersecurity behaviors into the education programs for business, law, social sciences, medicine, and other areas?* The understanding of technology, its promise and limitations, as well as the responsibilities in employing it, requires the inclusion of cybersecurity know-how into a wide range of disciplines.

For example, consider the field of social work, an area of specialization that employs almost 700,000 people in the United States and will add 100,000 additional professionals by 2026.[*] Social workers observe client confidentiality, maintain records protected by multiple regulatory regimes, and increasingly employ digital tools as enablers for productivity. The question we want to answer for it is: How does social work curriculum need to incorporate cybersecurity into professional preparation? This is a question in need of application *to many fields*.

Cybersecurity for Everybody?

When we start approaching how disciplines should incorporate cybersecurity into decision-making, professional responsibility, and leadership, there is obvious pushback on simply

exporting general cybersecurity knowledge from computer science and engineering. Professionals in myriad fields need to know what is relevant to them – starting with regulatory items that may be detrimental to certification or continued practice in a given field – but accepting the need for practical professional preparation on cybersecurity will require new modes of identifying, encapsulating, and delivering relevant critical knowledge. Expanding cybersecurity education and training efforts to a wider audience should include presenting relevant material in many majors and professional degree programs: business (including MBAs); law and social science; psychology; science; medicine; and engineering among others.

One answer on cybersecurity outside of traditional areas in academia has been to leave the problem to employers. This often translates to online annual training that likely has little impact on cybersecurity awareness and behavior.[†] Critical thinking on cybersecurity in preparation and lifelong learning for non-cybersecurity professionals is desperately needed, but rarely found inside most undergraduate disciplines or higher levels of education. Consider Symantec's lead healthcare technical architect's statement from just last year, who said of medicine, "[W]ith the exception of a few 'doctor-turned-geek' type of characters, I [have] never interacted with a doctor on cybersecurity – meaning those doctors whose main role is delivering care and who have not shifted gears into the IT or regulatory space."[‡]

What Needs Doing

There is an unmet need in understanding what and how much security knowledge is needed by professionals as their careers become increasingly influenced or shaped by information and computing technology. Unfortunately, most have little expertise in how to employ them responsibly with regard to cybersecurity. Even in computing disciplines, there has been considerable debate in how much cybersecurity thinking need be horned into undergraduate and graduate degree programs.

Where we need to advance cybersecurity is in engaging with other fields – business, law, medicine, and many others – to create meaningful professional preparation that can be built upon as cybersecurity evolves. This will mean engaging with disciplines across the university. The objective is not to make people in all disciplines cybersecurity experts, but rather deliver targeted awareness to issues that are within the context of their responsibilities. For instance, social engineering and phishing education is needed by all who use email. But understanding how email works is far less important than knowing how actions and behaviors are manipulated by others in the medium. The need is in incorporating cybersecurity behaviors or logics into daily work.

Expansion of cybersecurity elements into other disciplines curricula needs to be context aware, and user context behavioral based elements should address the following areas of interest:

- What skills and knowledge should people in any respective field have, and how should that be acquired?

- What are proper ways to address the mix of education methods, industry practice, and government needs over a lifetime of work?
- What elements are discipline specific and what may be generalized across many areas of professional activity?

An Education Agenda

Academia has long offered "physics for poets" courses in the sciences that explain to non-physicists' concepts of the discipline that may be helpful to know. While requiring that all students take an introductory cybersecurity course would be folly, we do know that some cybersecurity knowledge is a necessity for doctors, lawyers, program managers, civil engineers, social workers, retail managers, schoolteachers, and many, many other professionals. They need to know how to responsibly employ computing technology with regard to cybersecurity in the conduct of their professions.

What needs to occur is determining what knowledge regarding cybersecurity can be imparted within the context of the recipient's professional preparation and career path. We are not suggesting that all students become cybersecurity experts, passing the *Security+* exam or being able to speak intelligently on the Diffie-Hellman key exchange, but rather they learn what's needed through targeted curricula, preferably in courses that already exist. No doubt, skilled experts will be needed to assist the workforce in reinforcing organizational cybersecurity capacity, but more work needs to be done on security behaviors for professionals employing systems that may be attacked via cyber means.

The engagement needed is between cybersecurity programs and the other areas of education and professional preparation undertaken in colleges and universities. The task at hand is to engage with other academic programs on incorporating cybersecurity knowledge and behavior with appropriate, tailored content by discipline in the context of professional responsibility.

---

[*] "Social Workers." Occupational Outlook Handbook. Bureau of Labor Statistics, Washington, DC, available at: https://www.bls.gov/ooh/community-and-social-service/social-workers.htm.

[†] Bada, M; Sasse, A; (2014) *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* Global Cyber Security Capacity Centre, University of Oxford: Oxford, UK.

[‡] Wirth, Axel. "The Doctor Is In." *Biomedical instrumentation & technology* 51, no. 6 (2017): 514-517.

Cybersecurity automation and security

Susan G. Campbell and Petra Bradley, University of Maryland

The roles of future cyber professionals

The future of cybersecurity will be automated. Like less skilled personnel in other industries, less skilled cyber personnel are already being replaced by automated systems. Deep learning systems and other forms of artificial intelligence are being used for intrusion detection and network monitoring tasks. Straightforward tasks in other domains, such as secure programming, can be implemented using complicated but deterministic rules. Unlike humans, automated systems do not suffer negative effects from extended vigilance and do not accidentally omit procedural steps to create security holes. The current shortage of qualified cyber personnel should increase motivation to develop automated systems to fill holes in organizations' security postures that would otherwise have been filled by people.

Personnel who understand cybersecurity will still be required, because human decision-makers are needed to specify and build these systems, operate them, audit their operation, check them for security flaws, and provide them with training data. Cyber jobs of the future will encompass these areas rather than more routine actions, and people who are engaged in cyber work must also anticipate human and organizational behavior to mitigate human-generated security concerns. The roles of personnel in cyber will not necessarily change from the roles listed in the National Initiative for Cybersecurity Education (NICE) Cyber Security Workforce framework, but the way people do those jobs will change.

Future cyber education topics to support those roles

Security personnel will be required regardless of the level of automation that is achieved, but those personnel might focus their efforts on supervising automated processes and making decisions, rather than performing routine monitoring or defense.

Understanding human and organizational behavior

Future cyber personnel will need to understand which problems can be solved using technological means and which problems are due to the fact that organizations are made up of humans whose main priority is not generally security. Curricula need to increase cybersecurity

students' understanding of humans and sociotechnical systems (made up of people and technology), not just the technology.

Designing and evaluating automation

Other fields, as well as cyber, are building automated systems to accomplish tasks that do not need to be performed by humans to be successful. For example, goods that were once assembled by humans are now often assembled by machines, with human supervisors who ensure that the machines are working properly and who are equipped to trouble-shoot the systems when necessary. Cyber systems should gather best practices from other fields. Students who are planning to build systems should learn information security and networking concepts along with the appropriate kinds of automation (rule-based, machine learning based, or hybrid).

In addition to being able to build automated systems, organizations need personnel who are capable of evaluating whether automated systems are working properly and who can troubleshoot problems when necessary (or, at minimum, identify problems correctly so they can request the right kind of assistance). Generally, this requires understanding the systems and how they are meant to interact when they are working properly.

Operating systems and providing training data

Automated systems can reduce the number of personnel in certain roles within cyber, but any organization should have some way of evaluating whether their systems are working appropriately. This can be ascertained by inspection and monitoring of processes, or by challenging the system (e.g., conducting a "red team" exercise). In machine learning based systems, training data that are appropriately labeled and tagged can greatly accelerate the process of building and evaluating effective systems.

Operators may not need the skills to design automation, but they should be able to execute human-machine teaming tasks and identify malfunctions. Students who are planning to operate systems should have an understanding of the underlying mechanisms, but do not necessarily need to be able to build systems.

Securing the security software

The people who are most skilled at building automated systems may not be those who best understand security. Therefore, cybersecurity curricula should include a track for "pure" security, which would include evaluating automated systems as well as advancing the science of security.

Future-proofing cyber education

The realm of cyber is ever-evolving, and the types of threats to cybersecurity are likewise a changing landscape. Constant change presents a unique challenge; unlike topic areas in which our understanding of the basic truths has been constant for decades (or much longer), cybersecurity risks can change over a very short period. Deliberate human actions like denial and deception also co-evolve with defensive actions. One way to prevent curricula from "going stale" is to focus on basic understanding of human motivation and behavior. Although the actions and mitigations occur in a technological context, they are carried out by human actors whose actions can only be observed by their digital fingerprints. Understanding how people might exploit capabilities of new technology will help cybersecurity professionals to anticipate and understand the behavior they see on the systems they protect.

Author bios

Susan G. Campbell is an Assistant Research Scientist at the University of Maryland Center for Advanced Study of Language (CASL) and a Lecturer at the University of Maryland College of Information Studies (iSchool). Her current research focuses on determining and measuring the cognitive abilities required for different tasks within the cyber workforce. In addition to teaching a human-centered cyber course, she works on curriculum development for cyber across programs within the iSchool.

Petra Bradley (not attending) is an Associate Research Scientist at the University of Maryland Center for Advanced Study of Language (CASL). She is a cognitive psychologist interested in human learning and memory, decision making, and human-machine teaming. Her current projects focus on human trust of recommender systems and detecting insider threat. She has worked extensively with language and intelligence analysts to determine how they use information systems and what types of automated assistance can best benefit them in their work.

A new approach for Bachelor degree in Cybersecurity

Agnes Chan
Northeastern University

Introduction.

With the rise in demand for cybersecurity professionals, comes along a proliferation of training programs. These programs range from online training to traditional degrees, from certification to master degrees, all with the goal of producing qualified cybersecurity workforce within a short period. Unfortunately, with all the programs available to students, the gap between supply and demand in cybersecurity workers remains large. More troublesome is the feedback from potential information technology (IT) employers stating that the product of these programs is underqualified. In the 2015 survey report on Cybersecurity Job Market[1], published by Burning Glass Technology, a workforce study company in Cambridge, it was found that 37% of IT employers indicated that fewer than 25% of the graduates are qualified. This leads us to ask questions such as "What is missing in these programs?", "Are we providing the correct training at the right level?", or is it that in our haste of mass producing cybersecurity workers, we are skimming over the fundamental knowledge of the field? This white paper will discuss the weakness of current practices, and propose a new direction in training cybersecurity professionals.

Cybersecurity and Healthcare Professions.

Cybersecurity concerns the protection of computer systems and networks. It builds on the fundamental knowledge of computer science, such as coding, operating system and network. These topics should be taught with similar depth as expected in computer science. However, it differs from computer science in that it concerns the proper functioning of its protected entities, even when they are under attack, whereas computer science concerns the use of computers to achieve efficient computation and engineering designs. The concerns of the two professions are different, the goals and approaches of the programs should be different. Currently, most of the cybersecurity programs follow the methodologies of IT or computer science education, with modification in requirements by adding essential, non-technical knowledge such as cyber law

[1] ISACA State of Cybersecurity 2017: Current Trends in Workforce Development

and human interaction. One other significant modification is the requirement of laboratory exercises. While laboratory exercise in a course provides hands-on experience in learning a focused cybersecurity concept, it does not provide graduates with a holistic view of the problem or vulnerability itself.

On the other hand, while the technical training expected in cybersecurity and healthcare are vastly different, the objective of being able to detect and protect their clients are similar in both disciplines. Both disciplines require fundamental concepts, upon which their disciplines are built. Nurses require basic understanding of biology and chemistry, while cybersecurity workers require fundamental comprehension of coding, systems and networks. Nurses need to know how to communicate with patients, how to look out for suspicious decease, how to provide simple treatment plans, and know when to notify doctors. These skills are taught in courses such as nursing practices and, nursing care for children or adult patients. A cybersecurity professional may not need to communicate with users often, but he needs to be able to detect possible vulnerabilities, to discuss his findings clearly and succinctly with his cybersecurity teammates, and to explore a possible solution to mitigate losses. Current programs do not provide courses within the curriculum to teach cybersecurity students this needed skill, it is left to the students to pick up the skill set through post graduate work experience or other venues. To remedy this shortcoming of the curriculum, we propose the introduction of practicum courses in the last 2 years of their study. These practicum courses allow students to observe and to learn how professionals work as a team to solve problems; they may even learn to participate in decision making through professional mentorship.

Collaboration: Government, Industry and Academia.

Similar to Nursing programs, cybersecurity programs will not succeed without the collaboration from government and industry. In general, academia lacks the opportunity and facility to provide on field training to cybersecurity students. Government and industry are asked to take students on site, mentor them, show them how decisions are made and how one person's behavior affects the entire system. Opportunities for students to observe and to learn are crucial for the success in the education of a cybersecurity professional. In addition, these practicum courses can serve as work experience required by IT managers.

Cybersecurity is also getting more challenging every day, especially with the introduction of new technology and its ensuing applications. One such example is the Internet of Things (IoT). The communication complexity, together with the intricacies of the technology and network infrastructure, have posted new security and reliability challenges to cybersecurity professionals. As new technologies are introduced, the attack surface grows, so does the variation of attacks. It is difficult for a cybersecurity professional to familiarize himself with all the new technologies. These technologies have to be taught and transferred from government and industry experts to security professionals. In addition, with current shortage of qualified cybersecurity educators, government and industry can help narrowing the gap by allowing their employees to teach part-time in academia.

In short, government needs to create programs that fund industry/government professionals to partake in the teaching of cybersecurity. Industry needs to provide expertise and mentorship in training students. It is only through these collaborations that cybersecurity professionals can be well prepared to face the challenges, now and in the future.

Other Mechanisms to Strengthen Cybersecurity Education.

Other strategies that can strengthen the training of cybersecurity professionals include

- *Textbooks*. Textbooks provide a venue to define cyber security taxonomy uniformly. Furthermore, textbooks provide a certain standard of depth in each topic area.
- *Conferences*. Papers accepted or presented by security conferences should include tutorial on new industry technology and the security issues anticipated. Small group discussions on cybersecurity experiences, such as "A problem I encountered and how I handled it", should be encouraged and arranged in conference meetings. Students, especially the MS students, often attribute their learning from peers. The small group discussion is to facilitate peer learning experience.

The cybersecurity community has been debating for the last decade on what knowledge units are needed to be included in the education program. This debate needs to continue to ensure that cybersecurity professionals possess the needed knowledge. But transfer of knowledge is a relatively easy problem to solve. The teaching of professional behavior and experiences require more thought. We are proposing a new paradigm in educating cybersecurity professionals based on how they are expected to perform as a professional upon graduation.

Biography.

Professor Chan received her PhD in mathematics and joined the Northeastern University faculty in 1977. She is currently the Executive Director of Information Assurance and Cybersecurity. Her research focuses on cryptography and communication security. She works on fast, efficient mutual authentication algorithms for small mobile devices. More recently, she focuses on cybersecurity workforce. Professor Chan holds two patents on stream ciphers. She has published widely in IEEE conferences and journals, as well as in Crypto and Eurocrypt. Her research has been funded by NSA, NSF, DARPA and telecommunication industries. She was awarded the Distinguished Educator Award presented at CISSE in 2016.

Professor Chan led the effort in establishing an interdisciplinary research Institute of Information Assurance at Northeastern University. She is the PI for Center of Academic Excellence in Cyber Defense, Research and Cyber Operations. She designed and launched the interdisciplinary programs in cybersecurityat at Northeastern University: MS in 2005, PhD in 2010 and BS in Cyber Security in 2017. Professor Chan has been active in promoting women in sciences, in particular, she has participated as an invited speaker at NSA's "Women in Mathematics" and "Alumni Mathematicians" at Smith College.

I intend to share my ideas from an information science perspective to address the question that has perplexed cybersecurity researchers and educators: "How do we get more US citizens—and a more diverse population —into cybersecurity in meaningful ways?"

The smart innovations ranging from wearable devices to smart homes to cars to medical devices have become part of our daily life and continue to shape our behavior in the foreseeable future. According to 2018 Global Megatrends in Cybersecurity by Ponemon Institute, 82% of IT practitioners predicted a data breach from unsecured Internet of Things (IoT) devices is very likely to occur in the subsequent years. However, a recent cyber-security knowledge survey by Pew Research Center reported most Americans had limited cyber-security knowledge, which implies that those with smart devices connected to the Internet are at higher risks of cybersecurity threats. While most Americans have limited knowledge about cyber-security concepts (like strong passwords and risks of public WiFi network), most of them are unfamiliar with the key technical cyber-security concepts, such as botnet, VPN, and two-factor authentication (Olmstead and Smith, 2017). This reveals the fact that there is an urgent need to increase the cyber-security knowledge level of general public in the United States.

Extending Existing Stop-Think-Connect Model to a Complementary Education Model for the Public: Learn-Think-Change

"Leaning without thinking leads to confusion; thinking without learning ends in danger." ~ Confucius

In 2010, President Obama designated October as National Cybersecurity Awareness Month. The Department of Homeland Security (DHS) has initiated the national campaign and promoted partnerships between public and private sectors using the hashtag #cyberaware. Apart from that, a cybersecurity awareness program, entitled Stop-Think-Connect from DHS, has been adopted as a cybersecurity education model for community colleges (Fernandez et al., 2016). Inspired by this model, I suggest considering how learning and behavioral change theories/models can contribute to creating a complementary education model of cybersecurity literacy, namely Learn-Think-Change, for the general public.

(1) Learning Cyber-Security Knowledge and Public Opinion of Cyber-Security Awareness on Social Media

Many scholars have been investigating the professional knowledge trends in cyber-security research based on scientific research publications. However, few efforts have been put into mining user-generated content relevant to cybersecurity knowledge exchange on social media platforms. It would be meaningful to monitor the informal knowledge and resources shared through the hashtag networks in social media-enabled electronic networks of practice (eNoPs). eNoPs refers to geographically dispersed virtual communities with members who may never meet each other but share the same professional interests and publicly exchange information, advice or resources online. Social media enables eNoPs to informally exchange knowledge across boundaries in a timely manner (Beck, Pahlke, & Seebach, 2014). Taking the healthcare field as an example, Healthcare Hashtag Project is an open platform for connecting healthcare stakeholders (i.e., patients, caregivers, advocates, doctors and other providers) to timely information on Twitter. Hashtag networks link social media enabled eNoPs among professionals with diverse backgrounds to a variety of information resources, including questions and answers, news, hyperlinks, videos, images, and so on. I think it would be helpful to have one similar initiative, Cybersecurity Hashtag Project, for connecting cybersecurity stakeholders and communities through hashtag networks to organically create a substantial knowledge base. Such an initiative has the potential to engage and influence both cybersecurity curriculum across disciplines as well as life-long continuing education for the public.

(2) Thinking about Cybersecurity Risks and Risk Information Seeking

Cybersecurity behavior is always a choice. People can choose how they respond and react to cybersecurity challenges. What cybersecurity behaviors and choices will serve people best depends on their cybersecurity risk perceptions and how they view and cope with cybersecurity risks. Human information behavior could serve as a bridge to understand how people seek, process, and share cybersecurity risk information to bridge their information and knowledge gap. Integrating the concept of risk communication from the field of communication and information behavior from information science, the risk information seeking and processing (RISP) model (Dunwoody and Griffin, 2015) appears to be an appropriate framework to discuss the factors influencing how people seek and process risk information to bridge their knowledge gap. It is worth noting that information insufficiency and informational subjective norm are the significant predictors that drive people's risk information seeking through different information channels. Though the RISP model was originally developed to examine motivations behind information

seeking and processing behaviors on mass media, the recent studies have shifted the focus to social media. Therefore, cybersecurity professionals could use this model to rethink their role in educating the public and influencing other professionals about seeking and acquiring cybersecurity risk information. Leveraging the perceived social influence from social media could be a meaningful way to motivate the public's desire to be informed pertaining to cybersecurity risks. As a result, risk information seeking plays an essential role in motivating people to make corresponding changes when facing cybersecurity threats, thus leading to an informed understanding of cybersecurity risks.

(3) Changing Cybersecurity Information Behavior by Choice Architecture Design (Digital Nudge of Secure Online Behavior)

Cybersecurity incidents will change the ways in which the public responds to and communicates about cybersecurity risks. Raising the awareness and knowledge level of cyber-security is the first step to trigger the cybersecurity behavioral change. Various approaches can contribute to intervention design of cybersecurity awareness and literacy. The successful experience of motivating health behavior change using choice architecture may be replicated in the field of cybersecurity. From the perspective of behavioral economics, Thaler and Sunstein (2008) proposed the notion of choice architecture and defined it as the presentation of choices that nudge user decisions. Since choice architecture aims to affect behavior change without forcing people to accept but informing them of potential choices, it considers impact evaluations of informative presentations. In the digital world, the concept of digital nudge has been proposed to provide "a sort of compass to help individuals navigate a world of choices" (Schüll, 2016, p. 303). Similar to the IRS tax map built on semantic integration and topic maps, a cybersecurity map combining different knowledge mapping tools (e.g., mind maps, concept maps, and topic maps) could be developed. Such a map can assist users in searching and navigating cyber-security and privacy concepts by providing decision aids for their tasks relevant to changing the security and privacy settings of their smart devices.

Summary

Social influence through social media is one of the characteristics that we could leverage to change public perception and human information behavior about cybersecurity risks. Information

professionals can help design interventions using choice architecture to address users' information needs. This could mean designing effective information architecture for websites and mobile applications or providing an integrated knowledge mapping tool to facilitate learning and conveying cybersecurity concepts. In this way, users can learn where to find more cybersecurity information and locate their needed resources in a timely manner.

Author's Bio Sketch

Hsia-Ching Chang is an assistant professor in the Department of Information Science, College of Information at the University of North Texas. She is affiliated with the Center for Information and Cyber Security (CICS) at University of North Texas. She received her PhD and MS in information science from the University at Albany, State University of New York as well as her MA in public policy from the National Taipei University in Taiwan. Her research interests concentrate on cybersecurity, data analytics, social media, knowledge mapping, scientometrics, information architecture, and information interaction. She got the Cloud Security Alliance's CCSK (Certificate of Cloud Security Knowledge) certified, the first IT certification for secure cloud computing. She has been teaching the graduate-level course, Information and Cybersecurity, since 2015. She is the co-editor of the new book "Analytics and Knowledge Management" in Data Analytics Applications Series published by CRC Press, Taylor & Francis Group. She is currently co-editing a book entitled "Cybersecurity for Information Professionals" to be published by Libraries Unlimited, ABC-CLIO in 2019.

References

Beck, R., Pahlke, I., & Seebach, C. (2014). Knowledge exchange and symbolic action in social media-enabled electronic networks of practice: a multilevel perspective on knowledge seekers and contributors. *MIS Quarterly*, 38(4), pp. 1245-1270.

Dunwoody, S., and Griffin, R. J. (2015). Risk information seeking and processing model. In H. Cho, T. Reimer & K. A. McComas (Eds.), *SAGE Handbook of Risk Communication* (pp. 102-118). Thousand Oaks, CA: SAGE Publications.

Fernandez, B. R., Garcia, C. A., Capriles, J. R., Ford, W. & Mooney, C. (2016). Building Bridges: From NSF I-Corps to Community Colleges – Cybersecurity for All. *National Cybersecurity Institute Journal*, 3(2), 11-23.

Olmstead, K., & Smith, A. (2017). Americans and cybersecurity, *Pew Research Center*. Schüll, N. D. (2016). Data for life: Wearable technology and the design of self-care. *BioSocieties*, 11(3), 317-333.

Thaler, R. H., & Sunstein, C. R. (1999). *Nudge: Improving decisions about health, wealth, and happiness*. New Haven, CT: Yales University Press.

Resources to Meet Cybersecurity Education Demands

By

Balakrishnan Dasarathy, PhD
Professor and Program Chair, University of Maryland University College, Adelphi, MD
Email: Balakrishnan.Dasarathy@UMUC.edu

The mission of the University of Maryland University College (UMUC) is to improve the lives of adult learners by operating as Maryland's open university, serving working adults, military service-members, their families, and veterans across the United States, and around the world. UMUC serves over 80,000 students worldwide and is one of the largest distance-learning institutions in the world. We have eight different cybersecurity and related degree programs at the undergraduate and graduate levels with specializations in software security, network security, cybersecurity technology, policy and management, digital forensics and information assurance, and about 11,000 students are currently enrolled in these programs. To increase access to quality higher education in cybersecurity at affordable cost (at UMUC and elsewhere), it is imperative that we develop several resources nationally. Nationally-developed resources not only amortize the cost over several institutions, they also prescribe and enforce certain minimum standards. The resources we need fall into the following categories (The need for many of these resources exists in other disciplines as well, but the need is more acute in our field.):

- (Hands-on) Laboratory exercises
- Environments for laboratory exercises
- Content
- Assessment materials

Laboratory Exercises: This is one area, as a field, we have made a good bit of progress. I am particularly aware of three programs funded by NSF, all of high quality. SEED at the University of Syracuse is a comprehensive one with laboratory exercises in network, web, software, system and mobile security, and cryptography. The Cyber4All exercises at Towson University focus on secure coding. The third one, a recent one, from the Florida Center for Cybersecurity includes exercises on incident response, penetration testing and malware analysis. All these three projects do have content support, but the content is tied to their laboratory exercises. UMUC will be using several of these laboratory exercises in a new program on Cyber Operations. To meet our cyber

workforce needs, it is imperative that NSF and other agencies continue to support this type of laboratory development work and transitioning the output to institutions nationwide.

Environments for Laboratory Exercises: Many universities need a laboratory environment with 24x7 support. Currently, in spite of advances in cloud computing and virtualization technologies, having a reliable computing environment for student teaching, and sandbox for research and experimentation cannot be taken for granted. Emulab and environments based on Emulab such as the DeterLab are better at supporting experimental research than instructional exercises by a large number of students. Several states (see, for example, Virginia Cyber Range, Baltimore Cyber Range) now offer cyber ranges for their citizens to practice their cybersecurity skills, but they are in preliminary stages of development. Students, in general, require a lot of hand-holding and assistance with trouble-shooting. Students in digital forensics also require access to a local, physical laboratory, as certain segments of computer science, telecommunication & networking students experimenting new concepts in operating systems, virtualization and cloud computing.

Content: I believe this is next frontier in higher education. As we know, textbooks are expensive and often students need to buy more than one textbook for a course. Fields like ours are also changing rapidly, and as such, textbooks become outdated within a few years after their release. An online version of a textbook is generally cheaper and supports revisions more easily than the corresponding hardcopy of the textbook. However, online textbooks, controlled by DRM software, have many restrictions such as short time of usage (often till the end of a specific semester), limited amount of printing, and restrictions on the number of devices; moreover, they are hosted on proprietary platforms. UMUC has had successful experience going "bookless" since 2015/2016, as noted in the one of the 2018 College Jeopardy Championship tournament episodes! With the assistance of subject matter experts, I have experience in developing content for seven courses in information assurance/cybersecurity over a two year period in areas that include network security, intrusion detection, digital forensics, cryptography, cyberlaw and privacy, and software assurance. My fear is that no single institution will able to keep up with content development and updating all on its own. Apart from the government supplied resources, specifically from NIST, there are very few "open resources." For a resource to be truly open, it should meet these 5 R's: (1) retain (make and own a copy of the resource), (2) reuse (use the

resource in many places), (3) revise (adapt/modify), (4) remix (combine the resource with other resources), and (5) redistribute (share the resource). With truly open educational resources that are self-contained, an instructor can easily tailor the content for a session or an entire course. Our community and sponsors should be encouraging high quality content development for degree programs at various levels. The National CyberWatch Center' Digital Press and EBooks, funded by NSF, is a good start here. The center also develops laboratory exercises and curricula, but the focus of the center currently is on community colleges and associate degree programs. MOOCs are a good development here as well, but, by and large, the content from MOOC courses have Intellectual Property restrictions. Moreover, content from a MOOC course might be tied to a specific platform and may not be easily portable and tailorable.

There are two competing requirements faced by higher education in content development today. One is the use of multimedia for enhanced learning experience. The other is in meeting the requirements of the Rehabilitation Act (1973) and Americans with Disabilities Act (1990, amended 2008). The key concept behind these acts is equal opportunity. A resolution agreement with the US Department of Education establishes that students with disabilities must be: "able to obtain the information as fully, equally, and independently as a person without a disability." At the minimum, in the short run, UMUC is committed to providing meaningful text alternatives for any non-text content. Technologies are available today (see, for instance, Office 365: Accessible by design) to create content that can be accessed without barriers as well for creating content by those who are challenged in some ways. Expanding access is not only the right thing but also the smart thing to do in meeting our cyber workforce needs!

Assessment Materials: To produce cybersecurity knowledge workers rapidly, our cybersecurity programs need to be more "open." We should not be demanding credentials (e.g., B.S. in Computer Science with 3.0 GPA); we should only be requiring that specific competencies be met. We need tailorable tests/assessments for verifying competencies. A good model to follow here is that of CYBRScore. The CYBRScore Skills Assessment is mapped to the NIST-NICE framework and employs hands-on scenarios to test competencies for a specific work role. For example, their Cyber Defense Analyst assessment consists of assessments for competencies in protocol analysis, intrusion detection, incident handling, and vulnerability analysis. This CYBRScore assessment technology is, however, proprietary. We need open solutions!

The Future of Security and Privacy Education:
Incorporating Cybersecurity Law and Policy into Cybersecurity Curricula

Paula S. deWitte, J.D., Ph.D., P.E.
Assistant Director, Texas A&M Cybersecurity Center and
Associate Professor of Practice, Computer Science and Engineering Department,
College of Engineering, Texas A&M University
Paula.dewitte@tamu.edu

What new approaches are required in educating the next generation cybersecurity workforce? (1) We cannot educate and train the large numbers of cybersecurity workers required in the United States. The question becomes: *How do we increase the efficacy of those we do educate and train?* (2) We have relative smaller numbers of women and other underrepresented groups in cybersecurity: Similarly, the question becomes: *How do we increase opportunities?*

The Issues: It is unarguable that the evolution of law and policy lags technology development. Both poorly anticipate what *may* occur; rather, society implements new laws and policies in reaction to events. Before the disclosures by Facebook and Cambridge Analytica, most analysts did not expect additional privacy regulations in the United States now being considered. Another issue is a current case before the Supreme Court of the United States (SCOTUS), Carpenter v United States.[1] The long standing legal precedent is that law enforcement does not require a Fourth Amendment Search Warrant to obtain data shared with a third party such as phone logs (i.e., numbers called, time called, call duration, and locations of the parties) with a vendor (i.e., the mobile phone service provider). The SCOTUS decision, due early summer 2018, may require such search warrants based on arguments that the pervasiveness of technology such as smartphones has fundamentally changed the power of technology to be more invasive in areas that individuals have a "reasonable expectation of privacy." Both issues, although seemingly incongruent, are concerned with privacy and protecting individuals when sharing data, either through "apps" or the government. These issues require cybersecurity workers to be cognizant when new legal and policy rules apply.

[1] https://www.oyez.org/cases/2017/16-402

Nor is this confined to domestic law and policy. Cyberworkers need to be cognizant of evolving privacy frameworks such as the General Data Protection Regulation (GDPR) with, among other issues, extra-territorial jurisdiction, broadly defined personal data of "data subjects," and the recognition that many non-EU countries are implementing GDPR (e.g., Singapore, Mexico, Canada).

Students studying cybersecurity today will be the front-line for protection, detection, and response to cyber attacks. They will make decisions within constrained time periods; yet, they are being educated without substantial knowledge of either American or international law and policy. These cyberworkers will not have the luxury of contacting legal counsel for advice because of the sheer volume of decisions and the need for rapid action. What is required is academic curricula devoted to cybersecurity law and policy to develop students' capabilities to analyze and confidently apply emerging laws and policies without constant reference to legal advice.

Such courses are often mis-labeled as "soft skills" and treated as an after-thought rather than an integrated component of cybersecurity curricula necessary to support technical decision-making. Educating front-line protectors, defenders, and responders through tailored course content and pedogeological processes improve the efficacy of cybersecurity workers. This is a better approach than educating more cyber savvy attorneys. [Good luck with that!] This is misguided. It creates yet another legal specialty within the already burdensome, time-consuming legal process, and does nothing to address cyberworkers time-dependent performance requirements.

As students, legal savvy cyberworkers should:

1. Acquire the common body of knowledge for cybersecurity law and policy to include terminology, concepts, and specific legal terminology.
2. Acquire the common body of knowledge related to national and international laws related to cybersecurity and their differences.
3. Apply legal concepts in issues related to cybersecurity including cases/controversies unique to cybersecurity.

4. Identify and explain common legal issues related to cybersecurity.
5. Understand and explain procedural legal requirements relevant to cybersecurity.
6. Demonstrate the ability to use legal and policy knowledge by analyzing cybersecurity issues from a cyber worker perspective such as whether a security incident violates a privacy principle or legal requirement necessary for a valid response.
7. Demonstrate the ability to work through a case study identifying legal issues, analyzing the cybersecurity action required, and formulating a plan that complies with applicable laws.
8. Synthesize an action plan through analyzing cybersecurity legal and policy knowledge issues

Scope of the Issue and Analysis of the NIST NICE Framework: A search on the NIST NICE Framework using search terms of "legal;" "law;" "privacy;" "counsel;" "regulation;" "compliance'" "policy/policies" (an ambiguous term and used only in the context of government policies) "contract," "legislation," or "Executive Order," reveals a number of required tasks and KSAs throughout the seven Specialty Area Categories.

The initial analysis of the Framework found 72 tasks, 26 knowledge IDs, 6 skills, and 12 abilities that require some form of specific law and privacy knowledge. Although cursory , the analysis anecdotally identifies a surprisingly significant number of specialty areas requiring relevant KSAs for non-attorney work roles such as: (1) System Architecture (ARC): *"Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes." or* (2) Threat Analysis (TWA): "*Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities*."

Yet, only two work roles within the Specialty Area "Advice and Advocacy (LGA)" require a Juris Doctorate degree. The LGA specialty: "*Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain.*

Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings." The LGA specialty occurs in two work roles: (1) Cyber Legal Advisor (OV-LGA-001) who "*Provides legal advice and recommendations on relevant topics related to cyber law*; and, (2) Privacy Officer/Privacy Compliance Manager (OV-LGA-0021) who "*Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams*."

By comparison, many more work roles with their specialty areas require legal/policy knowledge such as: (1) "*Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy*." [K003]; (2) "*Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).*" [K0044]; or (3) "*Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations."* [K0107].

Workshop: We propose incorporating into the NACE Workshop a discussion on deriving the requirements for courses to address this substantial gap. The proposer taught the first-ever course at Texas A&M University in Spring 2018 addressing the need for legal savvy cybersecurity students. She proposes to offer that syllabus as a point of departure for the discussion. The workshop and its anticipated contribution to curricula development is essential to building analytical capabilities of future cyberworkers to operate within the dynamic and time constrained cybersecurity threat environment.

Additional Benefits: Developing these curricula may help to broaden the spectrum of applicable jobs and may increase the diversity of cybersecurity workforce. In addition to attracting those with engineering and IT skills, expanding the curriculum to develop legal and policy skills may attract students with different analytic and communication strengths, and as a result, both increase their number while improving the competency of the holistic workforce.

.

Paula S. deWitte, J.D., Ph.D., P.E.

Paula S. deWitte, J.D., Ph.D,. P.E., is both a Ph.D. in Computer Science and a licensed attorney in the State of Texas. She is a registered patent attorney with the United States Patent and Trademark Office (USPTO). She is one of less than 100 licensed Professional Engineers in the State of Texas in Software Engineering (SWE). She holds a Bachelors and Masters from Purdue University where in 2015 she was honored as the Distinguished Alumna in the Department of Mathematics, School of Science. She obtained her Ph.D. in Computer Science from Texas A&M University in 1989. She currently is the Assistant Director of the Texas A&M Cybersecurity Center and an Associate Professor of Practice in Computer Science and Engineering. Prior to joining Texas A&M University, she started several technology businesses. She most recently started two companies in oil and gas on a patented process in analyzing drilling fluids [US Patent US 8812236 B1] and has a patent pending through the European Patent Office (currently on review by USPTO) on incident response to a cybersecurity attack in the industrial control environment. She has mentored start-ups at Rice University OwlSpark and the University of Houston RedLabs. Before she joined Texas A&M University in July 2017, she was an Adjunct Professor at the University of Houston.

NACE Workshop
June 9-10, 2018
New Orleans, LA

The Role of Extracurricular Activities in Cybersecurity Education

In order to sustain the long-term needs of the cybersecurity workforce, more young people must be recruited to pursue cybersecurity-related careers. Career trajectories are often shaped early, even as early as middle school. It is therefore essential that more interventions and outreach efforts target these earlier age groups. Cybersecurity education is severely lacking at the primary and secondary school levels [1], and does not appear to be improving in any significant and widespread way. Most K-12 schools around the country are over-tasked and under-funded, and there is little room for new programs. While the "CS for All" initiative has gained some traction lately, it has been, and continues to be, a long uphill battle. It is unlikely that cybersecurity will ever be able to evoke the same broad appeal as an academic subject, and cybersecurity will almost certainly remain a rare subject in American primary and secondary schools for the foreseeable future. Therefore, the best way to introduce these young students to cybersecurity topics and careers has to be outside the classroom, with extracurricular educational activities.

Studies have found that extracurricular activities can have a significant impact on students' educational and career choices, and they can be an effective avenue for stimulating interest in specific career fields. Competition-style activities have been particularly successful at getting more students interested in STEM careers. A study of past participants in the National Ocean Sciences Bowl, for instance, found that 41% of respondents indicated that participation influenced their choice of career, and 39% said that it influenced their choice of college major [2]. Extracurricular competitions can also help launch talented students into highly successful careers. Winners of academic Olympiad competitions were found to significantly outperform their peers in various measures, and both participants and their parents agreed that the Olympiad developed their talent and fostered their future accomplishments [3]. These types of activities can help motivate students to pursue a subject and/or career, and to strive for excellence in that field. The activity can serve as an impetus to get the student started, and to help drive them toward

success when they get bored or frustrated. These activities also foster role-model relationships between professionals, who often serve as mentors and judges, and the students participating. Meaningful interaction with "real" practitioners can have a powerful impact on a young person. This is especially important for students who do not often receive exposure to a wide range of careers, and to students who may have difficulty seeing themselves in a particular career because their race or gender is underrepresented [4].

It is encouraging that competition-style extracurricular activities have been successful in other STEM fields, since competitions are already one of the most popular forms of cybersecurity activities. There are now dozens of cybersecurity competitions, both large and small, for varying skill levels [5]. One of the most popular is the Collegiate Cyber Defense Competition (CCDC), a national cybersecurity tournament for college students, with affiliated regional competitions [6]. CCDC has gained popularity especially for its value in creating hands-on learning experiences for students in cyber and computing related fields. It also has the potential to increase the inflow of new students into the cybersecurity profession, by recruiting, retaining, and identifying students who would be interested and adept in cybersecurity roles [5], [7].

As discussed earlier, however, college is too late for many students, who may have already chosen a different career path. It is important, therefore, to provide opportunities below the college level. The only truly national program of cybersecurity extracurricular activities for middle and high school students is CyberPatriot [5], [8], run by the Air Force Association, CyberPatriot bills itself as "The National Youth Cyber Education Program" [9]. The central element of the CyberPatriot program is the annual cyber defense competition, in its tenth season as of the 2017-2018 school year. Small teams of middle or high school students scour a virtual computer for vulnerabilities, such as viruses, backdoors, and incorrect security settings, then eliminate those vulnerabilities for points. These teams can come from public or private schools, homeschool groups, Junior ROTC programs, Civil Air Patrol units, or other approved youth organizations [8], [10], [11]. A recent study [12] demonstrated that participation in the CyberPatriot program leads to increased interest in cybersecurity as an educational or career prospect. Furthermore, that increased interest was found to persist over time, leading to significantly increased likelihood of actually entering the cybersecurity workforce. The CyberPatriot program is also contributing positively to correct the gender imbalance in the

cybersecurity workforce. Female students consistently make up over 20% of the competition–approximately double the industry average [13]–and despite lower initial interest in cybersecurity careers among female participants, this interest increased by an even greater amount than it did for males.

In addition to CyberPatriot's national program, there are many excellent extracurricular programs springing up around the country. Many colleges, universities, and other organizations host locally-organized cybersecurity camps for local students and/or teachers. These camps are often supported by GenCyber [14], a joint National Security Agency and National Science Foundation grant program that enables select camps to be offered free to participants. There are also numerous small, independent non-profit groups offering a variety of programs to local youth, based on the passions of their volunteers and the availability of donor funding. Examples of such programs include Cyber Warrior Princess (www.cyberwarriorprincess.org) in Ohio, GhostWire Academy (ghostwireacademy.org) in Texas, and many others. These programs and others like them give young people opportunities to delve deeper into cybersecurity, opportunities they would not have had through traditional education systems.

Another approach for using extracurricular activities to introduce young people to cybersecurity is to incorporate cybersecurity content into existing youth programs. Civil Air Patrol and multiple Junior ROTC programs have done this very successfully using the CyberPatriot competition. The Girl Scouts of the USA have recently announced their plan to introduce a series of age-appropriate cybersecurity badges to their programs. This is a great example of how other youth programs can add cybersecurity to their offerings as well; in fact, Scouting badges are frequently cited as the prime model for using badging to motivate learning [15], [16]. The Boy Scouts of America has a program for personal online safety education [17], though nothing currently for cybersecurity. A team of professionals and educators is working to change that by designing and proposing a new Cybersecurity merit badge [18]. The great advantage of incorporating content into well-established youth programs is the breadth of the audience. Participants in these youth programs often try different activities just because they are offered by the organization (and maybe to earn a badge), potentially setting them on a path toward a career they would not otherwise have considered.

Extracurricular activities are establishing themselves as the centerpiece of cybersecurity education for American middle and high school students, and this trend is likely to continue. It is

critically important that the cybersecurity community as a whole embrace and support these programs, and they should be considered a central aspect of the overall strategy for K-12 cybersecurity education.

References

[1] G. L. Peterson and B. J. Borghetti, "K-12 Cyber Security Educational Content Information Gathering," 2015.

[2] K. Bishop and H. Walters, "The National Ocean Sciences Bowl: Extending the Reach of a High School Academic Competition to College, Careers, and a Lifelong Commitment to Science," *Am. Second. Educ.*, vol. 35, no. 3, pp. 63–76, 2007.

[3] J. R. Campbell and H. J. Walberg, "Olympiad Studies: Competitions Provide Alternatives to Developing Talents That Serve National Interests," *Roeper Rev.*, vol. 33, no. 1, pp. 8–17, Dec. 2010.

[4] M. A. Ozturk and C. Debelak, "Affective Benefits From Academic Competitions for Middle School Gifted Students," *Gift. Child Today*, vol. 31, no. 2, pp. 48–53, 2008.

[5] Katzcy Consulting, "Cybersecurity Games: Building Tomorrow's Workforce," 2016.

[6] "National Collegiate Cyber Defense Competition," *National Collegiate Cyber Defense Competition*, 2017. [Online]. Available: http://www.nationalccdc.org/. [Accessed: 02-Mar-2018].

[7] P. Pusey, M. Gondree, and Z. Peterson, "The Outcomes of Cybersecurity Competitions and Implications for Underrepresented Populations," *IEEE Security & Privacy*, vol. 14, no. 6, pp. 90–95, 2016.

[8] G. B. White, D. Williams, and K. Harrison, "The CyberPatriot National High School Cyber Defense Competition," *IEEE Security & Privacy*, vol. 8, no. 5, pp. 59–61, 2010.

[9] Air Force Association, "Air Force Association's CyberPatriot: The National Youth Cyber Education Program," 2017. [Online]. Available: http://uscyberpatriot.org/. [Accessed: 20-Nov-2017].

[10] G. B. White, D. Williams, and K. Harrison, "Developing a National High School Cyber Defense Competition," in *CISSE '10 - Proceedings of the 14th Colloquium for Information Systems Security Education*, 2010, pp. 83–89.

[11] CyberPatriot Program Office, "CyberPatriot X: National Youth Cyber Defense

Competition Rules and Procedures." The Air Force Association, Arlington, VA, 2017.

[12] M. H. Dunn and L. D. Merkle, "Assessing the Impact of a National Cybersecurity Competition on Students' Career Interests," in *SIGCSE '18 - Proceedings of The 49th ACM Technical Symposium on Computing Science Education*, 2018, pp. 62–67.

[13] Frost & Sullivan, Center for Cyber Safety and Education, (ISC)2, and Executive Women's Forum on Information Security Risk Management & Privacy, "The 2017 Global Information Security Workforce Study : Women in Cybersecurity," 2017.

[14] "GenCyber," 2017. [Online]. Available: https://www.gen-cyber.com/. [Accessed: 31-Dec-2017].

[15] S. Deterding, "Gamification: Designing for Motivation," *Interactions*, vol. 19, no. 4, ACM, pp. 14–17, Jul-2012.

[16] B. Alberts, "An Education that Inspires," *Science (80-.).*, vol. 330, no. 6003, p. 427, 2010.

[17] Boy Scouts of America, "Cyber Chip." [Online]. Available: www.scouting.org/cyberchip. [Accessed: 15-Nov-2017].

[18] M. H. Dunn, R. J. Caruso, L. D. Merkle, and R. Trygstad, "Proposed Cybersecurity Merit Badge for the Boy Scouts of America (Poster)," in *SIGCSE '18 - Proceedings of The 49th ACM Technical Symposium on Computing Science Education*, 2018, p. 1085.

Author Bio

Michael H. Dunn is a cyberspace operations officer in the United States Air Force. He received a Bachelor of Science in Computer Science, with a specialization in Information Security, from the Illinois Institute of Technology (IIT), and a Master of Public Administration from IIT's Stuart School of Business. He was recently awarded a Master of Science in Cyberspace Operations from the Air Force Institute of Technology, where his research focused on the impacts of extracurricular cybersecurity youth activities.

Michael's Air Force career has included assignments at Creech Air Force Base (AFB) and Nellis AFB, Nevada, Wright-Patterson AFB, Ohio, and a deployment to Al Udeid Air Base, Qatar. He is currently assigned to the 333rd Training Squadron at Keesler AFB, Mississippi, as an instructor for Undergraduate Cyber Training.

In addition to his academic credentials, Captain Dunn also holds multiple information security certifications, including Certified Information Systems Security Professional (CISSP) and GIAC Certified Incident Handler (GCIH).

Co-Op Light:

Developing a Cyber Security Workforce through Academia-Industry Partnerships

The need for cyber security professionals in the workforce will only continue to increase and the existing shortfall widen (Fourie et al., 2014). There are not enough people to fill the open positions. Yet, there are individuals with an educational background in cyber security that are not being hired. They do not have the required experience in many cases (Caldwell, 2013). Thus, we see organizations struggling to fill positions in cyber security, but unwilling to hire those without experience. Coincidentally, these individuals will never obtain the experience in cyber security if some employers do not take a chance on them.

Some programs have been able to address this problem directly, such as the NSF's Scholarship for Service (M. E. Locasto, Ghosh, Jajodia, & Stavrou, 2011). It provides students with an opportunity to work for a governmental organization performing cyber security work in exchange for a commitment by the student to work for the organization for a certain number of years. The program has been very successful. However, it is not an attractive option for every student since the service commitment may seem too long for some or the pay too low.

Internships have also been available for some, but generally are more difficult to find as employers are reluctant to hire individuals with little or no experience, even for internships. Some students may end up performing cyber security related work in a computer science or information technology internship, which may later be leveraged for a more cyber security focused position within the same or a different organization. Although for those seeking a cyber security internship in the first place, this is not necessarily an efficient or effective pathway.

Therefore, new approaches are needed for cyber security, including the increased use of older approaches that have proven track records in other disciplines. One approach that has been effective has involved partnerships between universities and industry. An example of this being done at a high and intricate level is Northeastern's Co-op program that requires students

to alternate between semesters of academic coursework with semesters of co-op experiences. This typically begins the second semester of their sophomore year. Although highly successful and a model of effective co-op education, it does require a significant amount of coordination, relationship building with industry partners, and an institutional willingness to transform the educational structure of a university. Northeastern has been doing it this way for years and it works for them (Smollins, 1999). For other universities without this history, there may be significant bureaucratic and institutional hurdles to develop a co-op model for just one or more programs. Likewise, it can take several years to develop the necessary relationships, both within the institution and with external partners.

An effective approach for many universities may try and combine elements of internship programs with those of a co-op model to provide a more holistic educational approach to cyber security workforce development (Hoffman, Burley, & Toregas, 2012). One could think of this as "co-op light." This approach has been employed at some universities (M. Locasto & Sinclair, 2009), as well as the University of Washington under the coordination of the Center for Information Assurance and Cybersecurity (CIAC). During the initial stages of the development of this program, the University of Washington has partnered with a large corporation that has its headquarters in the region. This corporation has significant needs for diverse cyber security talent, including both technical and non-technical positions available.

To garner interest with potential participants, various information sessions are held on campus, such as the University of Washington Bothell campus. Given the diverse nature of cyber security positions available with this corporation, it is often a matter of finding the right fit between a unit or division of the corporation and high-caliber students. In other words, students apply to participate in the program. Various hiring managers within the corporation that represent these diverse units or divisions then look through the applicants to see if there is a specific fit for their needs. This approach helps maximize the experience for both the student and the corporation.

CIAC provides a point of contact for all participants that serves as a professional career advisor to them. If issues should arise, this individual helps troubleshoot them on behalf of the

student. Additionally, a cohort model is employed that allows for shared experiences between students as they enter the various components of the program together. This provides a peer-support mechanism for these students that can be invaluable.

Part of this cohort model includes the completion of additional academic coursework together. This three-course sequence results in a cyber security-related certificate from the University of Washington's Professional and Continuing Education (PCE) component. It also satisfies the requirements of CNSS 4011, CNSS 4012, and CNSS 4016. Thus, students walk away from this program with an additional credential and valuable work experience. For most, this has resulted in job offers for the student from the corporate partner with most of these offers being accepted. This is a win-win for the student and corporate partner.

Thus far, this program is in the process of completing its second cohort with the third cohort on the way. Part of the design of this program involves feedback from stakeholders and participants on a regular basis so that improvements remain ongoing and continual.

Several lessons have been learned and are continually being adapted and applied. For example, the three-course sequence that results in a certificate from PCE was a pre-existing certificate program that was not designed with the unique needs of program participants in mind. One possibility for the future may involve designing a certificate program that is custom designed for these students. The original decision to use a preexisting certificate curriculum was made to optimize the use of existing resources and to minimize program overhead, especially when the success of the model remained uncertain. As the program continues to demonstrate a successful overall approach, the development of a tailor-made certificate curriculum should be revisited.

Additionally, the program currently has one corporate partner. New corporate partners are being explored to build upon these initial successes. Diversification and expansion of corporate partners will be vital to ensuring the continued success of the program and provide a broader number of industries students with an interest in cyber security can pursue.

This program does not replace other successful programs, such as Scholarship for Service or full co-op models (e.g., Northeastern). Nonetheless, it does help fill a void. It provides greater flexibility as is often seen in internships, but with increased structure, learning opportunities, and a cohort approach, as is often seen in co-op models. The overall risk in participating in the program, whether as a student or as a corporate partner is also quite low compared to other models that have been employed in the cyber security domain. There will never be a one-size-fits-all approach to address the significant shortage in the cyber security workforce. However, by continuing to be creative and willing to take chances, additional voids can be filled and successes recorded.

References

Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud & Security*, *2013*(7), 5–10.

Fourie, L., Pang, S., Kingston, T., Hettema, H., Watters, P., & Sarrafzadeh, H. (2014). The global cyber security workforce: an ongoing human capital crisis. *Global Business and Technology Association*.

Hoffman, L., Burley, D., & Toregas, C. (2012). Holistically building the cybersecurity workforce. *IEEE Security & Privacy*, *10*(2), 33–39.

Locasto, M. E., Ghosh, A. K., Jajodia, S., & Stavrou, A. (2011). The ephemeral legion: producing an expert cyber-security work force from thin air. *Communications of the ACM*, *54*(1), 129–131.

Locasto, M., & Sinclair, S. (2009). An Experience Report on Undergraduate Cyber-Security Education and Outreach. In *Proceedings of the 2nd Annual Conference on Education in Information Security (ACEIS 2009), Ames, IA, USA*.

Smollins, J.-P. (1999). The making of the history: Ninety years of Northeastern co-op. *Northeastern University Magazine*, *24*(5), 19–25.

New Approaches to Cybersecurity Education (NACE) Workshop
Contact: Michelle Duquette duquettem@battelle.org 703-831-7413

Idea Submission

In order to address the shortage of a future cybersecurity workforce shortage, our efforts need to be focused on addressing the broader issue of technology education among our students. While children and young adults are presented with a multitude of electronic devices at home and in the classroom, the understanding of 'how' these devices work is lost. Without an understanding of 'how', how can we expect there to be understanding of the complex interactions and interdependencies within cybersecurity?

A video on YouTube, "*Teens React to 90s Internet"* with over 16 million views[1], depicts young adults experiencing an educational video about the Internet. They were asked questions about the meaning behind ".com" and ".org", and "How do you get on the Internet?" The young adults simply do not know how the Internet exists but simply that it is "just there." In addition to the problem of young adults not being taught, is the lack of technology teachers and curriculum to address the subjects.

I am proposing a mix of technical and non-technical topics discussed as part of every grade from elementary through high-school that advances in understanding and application as students progress. Younger grades are introduced to appropriate behavior, anti-bullying as part of activities that teach children right versus wrong; middle grades are focused on the parts and pieces that make up computers and the Internet, their functions and interdependencies; senior grades focus on theory, law, psychology and advanced certification studies.

Elementary / Grades 1-5

- Introduction to technology and appropriate behavior
- Game design through basic coding
- Cyberbullying

Middle school / Grades 6-8:

- Introduction to computer parts and pieces

[1]*Teens React To 90s Internet*, Published 01 June 2014 by REACT https://youtu.be/d0mg9DxvfZE

- Design theory through hardware deconstruction
- Technical drawing and network design

High-school / Grades 9-12:

- Combining the human element and technical function.
- Educating on landmark technical cases involving privacy (FBI Stingray), Computer Fraud and Abuse Act (CFAA)
- Historical figures (Alan Turing, Vint Cerf, Grace Hopper) and their contributions to computers and the Internet
- Workforce needs and education/certification requirements

In my work with high-school and college interns is the idea that "it's too hard" or, "it's not relevant to me" would consistently arise. Having been presented with topics such as the privacy control settings for popular smart phone apps, understanding what data types are generated from their interactions online and the value of that data, and even providing demos of hacks used via Wi-Fi, lead them to become more engaged on the subject and understanding that it does affect them and their everyday actions. Additionally, that the material was not difficult, only that they had yet to be presented with the information in a manner that was consistent with how they digest it (both visually through delivery and writing style).

While this level of interaction may not be possible to all students, I recommend a partnership with organizations that can provide the tools and resources to our education system. ISC^2 provides cyberbullying education directly with students, Palo Alto provides cybersecurity education to young girls through Girls Scouts while Disney, Khan Academy, and Tynker (among others) support 'Hour of Code' programs.

These programs are provided freely by both non-profit and commercial companies as part of a broader understanding of the need to teach our students these valuable skills. I propose requiring a larger commitment from commercial, non-profit and academia to provide education and training classes to high school students on cybersecurity. As students prepare to join the workforce, each individual is responsible for practicing 'good cyber hygiene' and it is within

these organization's best interests to ensure the next workforce understands their role and responsibilities to their employer regardless of their job title. It is also within these organization's best interest to interact with students on ethics, intellectual property, data breaches, risk management and consumer protections and privacy.

BIO

Michelle Duquette is a cybersecurity advisor supporting Government clients and Fortune 500 companies for over 10 years. Michelle has worked with integrated product teams and advised senior leaders on the issues of security engineering, Cybersecurity policy management, and information risk management across varying government classification levels. Michelle works as a Cyber Security Advisor with Battelle Memorial Institute and previously as a Senior Consultant for Booz Allen Hamilton, and a Software Engineer with Lockheed Martin.

Michelle holds both a M.S. in Computer Science and a Graduate Certificate in Information Assurance and Cybersecurity from George Washington University, and a B.S. in Information Management and Technology from Syracuse University. Michelle is a Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH). Michelle presented at the 2015 American Petroleum Institute 10th Annual Cybersecurity Conference on, "Biometrics: What is it and Where Do I Begin?"; published internationally in the July 2014 Information Systems Security Association Journal, "Our Children's Future: As Determined by Their Online Identity", and on the panel for TechWeekDC 2017 for 'Women Take on Careers in Tech' providing insight on how to start a career within cybersecurity in DC, perspective on how to create the career you want, and personal experiences.

Proposed College Curriculum Changes for Producing Secure Developers

Christine Fossaceca
MIT Lincoln Laboratory
christine.fossaceca@ll.mit.edu

The need for more robust software is evident from the increasing number of cyberattacks occurring daily. [1] However, the fear of sophisticated nation-state actors and zero-day vulnerabilities is partially misplaced. Although these are formidable enemies, companies and governments should be more concerned about a major threat from the inside: poorly constructed code. A search of the 2017 CVE database shows that there are still new buffer overflow vulnerabilities being found [7], despite those being among the most basic type of exploits. This leads to the question: Why are developers still implementing programs with simple vulnerabilities?

The first place to look may be the educational background of software developers. One major problem is that students who want to become software engineers see cybersecurity related courses and think, "That doesn't apply to me". Then those students become developers, leaving security concepts to be implemented by a "security team". Security researcher Sarah Zatko gave a presentation [5] at the Hackers of Planet Earth (HOPE) Conference in 2014 diagnosing this systemic issue as "security afterthought syndrome", and lamented that cybersecurity isn't prioritized by many professors or taught by universities. Two years later, Professor Ming Chow of Tufts University and his colleague, Professor Roy Wattanasin of Brandeis University, replied to Zatko at HOPE 2016 [3], where they discussed being inspired by her presentation and made changes on their own campuses to address cybersecurity in computer science education.

In order to determine if other colleges and universities were following the urgings of experts in the security community by making curriculum changes, I recently conducted a survey of over 100 colleges and universities in the United States and presented the results at the IEEE Secure Development (SecDev) Conference. I worked with two of my interns at MIT Lincoln

Laboratory, and we reviewed the Computer Science curriculums of select schools, which were chosen based on their US News and World Report Rankings [6]. The schools were in the 2017 listings for "Top 50 Nationally Ranked", "Top 50 Regionally Ranked", and "Top 50 Computer Science Programs".

In the first part of the research, we looked at every curriculum and course description, searching to see if any required courses had the word "security" in the description. We found that 97 percent of computer science programs had at least one course that mentioned the word security in the description, however, only 31% of schools actually required one of those courses in their curriculum. Furthermore, it was determined that the word "security" is too ambiguous to rely on as a metric, as word "security" meant cryptography, network protocol security, privacy, forensics, or cyber policy, just to name a few categories discovered in the survey.

In the second part of the survey, we looked at the accreditations of the schools, and noted that the majority of top tier schools were ABET accredited (50% of Regionally Ranked schools, 92% of Nationally Ranked schools, and 94% of the Top Computer Science schools). This suggests that the ABET committee drives the curriculum requirements for these schools. A search of the ABET computer science curriculum turns up a requirement for computer science programs, "To have an understanding of professional, ethical, legal, security, and social issues and responsibilities." [4] Although some schools didn't have ABET accreditation, they usually had another accreditation listed on their website, and their curricula were quite similar to those of the ABET schools.

We are producing more software than ever before, in a landscape where there are also more malicious actors, so most software developers unknowingly have a target on their backs. We have to start preparing college students to enter the increasingly adversarial environment of the Internet by building security concepts into computer science and engineering education. Although there will always be new kinds of cyberattacks, computer science students should be well-informed about old attacks. As an example, students who are learning C programming should not be taught to use strcpy() without learning what a buffer overflow is. This issue was addressed in 2010 by three Carnegie Mellon professors who were planning to implement

changes in the Computer Science curriculum to increase "our emphasis on the need to make software systems highly reliable." [2] Today, freshmen at Carnegie Mellon do, indeed, learn buffer overflow vulnerabilities in the required course 15-222 Principles of Imperative Computation, where students focus on the "correctness of programs", not "security".

I assert that graduating computer science students who go on to become software developers without learning secure coding practices ahead of time are left to learn on the job, and when a more experienced developer isn't auditing their work, another simple bug is implemented in production code, waiting to be discovered by the adversary. It is proposed that more schools follow the model of Carnegie Mellon in teaching secure programming techniques. To do this, reaching out to accreditation establishments and advocating for changes in curriculum requirements is necessary, as well as promoting the use of phrases such as "correctness of code" and "expected execution" rather than the vague word "security". This will in turn produce graduates who will be less likely to write programs with commonly known vulnerabilities.

References

[1] 2017 Internet Security Threat Report. Symantec Corporation, Apr. 2017, www.symantec.com/security-center/threat-report.

[2] Bryant, Randall E., Sutner, Klaus and Stehlik, Mark J. "Introductory Computer Science Education at CarnegieMellon University: A Deans' Perspective." Aug. 2010, www.cs.cmu.edu/~bryant/pubdir/cmu-cs-10-140.pdf.

[3] "Computer Science's Curricula Failure-What do we do now?" Chow, Ming and Wattanasin, Roy. HOPE 2016

[4] "Criteria for Accrediting Computing Programs, 2017-2018." *ABET*, Accreditation Board for Engineering and Technology, 2017, www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2017-2018/.

[5] "How to Prevent Security Afterthought Syndrome". Zatko, Sarah. HOPE 2014

[6] *Rankings and Advice*. U.S. News & World Report, 2017, www.usnews.com/rankings.

[7] Security Vulnerabilities Published In 2017." CVE Details Search, MITRE Corporation, 2017, www.cvedetails.com/vulnerability-list.php?vendor_id=0&product_id=0&version_id=0&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=2017&month=0&cweid=0&order=3&trc=9201&sha=815cc1a3d2c4b72bf23b8a2fa85939f5ab0041c0

Bio

Christine Fossaceca is a cybersecurity researcher at the MIT Lincoln Laboratory, focusing on tool creation, exploit development, vulnerability research, and reverse engineering. She first became interested in cybersecurity education when she entered the workforce as a recent graduate and started feeling overwhelmingly unprepared to write "unhackable" code. In speaking with other recent graduate friends, she noticed a trend among software developers to rely heavily on "security teams" to pentest their code for them in the deployment process, rather than the developers themselves following any particular set of secure coding practices. In her discussions, the nervous laughter of her colleagues usually covered up a real fear of causing a major security breach because the review team didn't patch something. She started to question, "Why did my professors even teach me strcpy()? Why didn't the databases course include a section where we tried to perform SQL injections on our classmates? Why didn't any of my classes encourage me to use a debugger like gdb?" After becoming interested in the topic, she became involved with the IEEE Secure Development conference (IEEE SecDev) and formed a group on improving security education with collaborators from Google and Tufts University.

Improve Cybersecurity Education by Bringing Secure Coding to CS1

New Approaches to Cybersecurity Education (NACE) Workshop, June 9 & 10, New Orleans, LA

Simson L. Garfinkel

The United States is utterly dependent on information technology, but only a fraction of the those working in computing specialize in cybersecurity. The reason is that the field of computing is tremendously broad. Just as there are now dozens of cybersecurity specializations, there are now dozens of computing specializations as well.

Consider the numbers from the 2016 Taulbee Survey, the annual survey by the Computing Research Association that tracks PhDs in computer science, computer engineering and information.[1] Of the 1888 students graduating in North America with a relevant PhD in 2016, just 106 (5.6%) found employment in "security/information assurance" — yet "security/information assurance" was the second largest employment category reported on the survey (only exceeded by Artificial intelligence). There are simply too many aspects of computing systems that require teaching and researching: security is critical, but so are the other specializations.

If our goal is to improve the state of cybersecurity using the lever of education, then we must consider ways of broadening cybersecurity education to include non-specialists. That is, we need a longer lever. This means incorporating security education throughout the entire computing curriculum, starting with the first computer science course that students take, affectionately called CS1 in the literature.

It has long been observed that many CS1 courses have programming examples that contain serious, exploitable security errors. In the days of "C" it was common for instructors to present programs with buffer overflow errors. These days, it is common to present programs that allow for brute-force password guessing, or SQL injection attacks, or just horrible usability that promotes unsecure use. We also have poor security practices in many educational computing environments—such as easy-to-guess passwords, open services, web services protected by hidden URL, and so on—in the interest of expediency.

[1] https://cra.org/crn/wp-content/uploads/sites/7/2017/05/2016-Taulbee-Survey.pdf

Programming examples with vulnerabilities and poor security practices in these introductory courses is poor pedagogy. We shouldn't be teaching the students with practices that we wouldn't want them to repeat on the job. We must scrub introductory courses of poor examples, and instead assure that these courses demonstrate good security practice. This will almost certainly require that security faculty partner with other faculty who teach the introductory courses.[2] [3]

As the need for programmers continues to expand, programmers who do not have the benefit of formal security instruction will be creating most of the code that powers our society. These programmers will use the tools of their trade. If introductory courses incorporate sophisticated security technology, it will be reflected in popular tools, there will be a multiplier effect. The result will be more code with fewer exploitable defects.

Other modern software engineering practices have been incorporated into introductory courses with great success, including test-driven development, continuous integration, and distributed source code control. These practices have been adopted because they make programmers more efficient and decrease software defects—and in the process, help to make software more secure.

Likewise, introductory programming courses should teach code annotations to support model checking, the use of static code checkers, and lightweight formal methods.[4] These techniques will be sold to students (and their teachers) as ways to make software more reliable and software development more efficient. As a side effect, their code will also be more secure.

April 26, 2018

[2] K. Nance. "Teach them when they aren't looking: Introducing security in CS1." IEEE Security and Privacy, 7(5):53–55, Sept. 2009.

[3] V. Pournaghshband, "Teaching the Security Mindset to CS 1 Students," SIGCSE'13, March 6-9, 2012, Denver, CO.

[4] K. Schaffer, J. Voas, "Whatever Happened to Formal Methods for Security," IEEE *Computer,* August 2016.

Integrating Cybersecurity into the K-12 Classroom

We are living in the midst of a social crisis as technology rapidly expands and bad actors take advantage of our democratic system. America's belief in the power of liberty and open systems comes with drawbacks such as opposition to preemptive, offensive, or aggressive actions taken in the field of cybersecurity by our own government officials. Achieving the balance between liberty(privacy) and security is a challenge. As a country we should strive to "future" proof the education provided in cybersecurity. To achieve this worthy goal an emphasis on teacher development and an intentional expansion of resources into the K-12 environment must occur. A job shortage of a predicted 1.8 million people by 2022 (CSO Online, 2015) and the increased need to teach digital natives basic cybersecurity survival skills, (Irish Times, 2018) require that cybersecurity be integrated in a multidisciplinary fashion in the K-12 classroom. Educating the populace in the field of cybersecurity is necessary for three concrete reasons: 1. To prepare students for an ever-increasing technology-based future; 2. To expose students to the jobs and careers available in cybersecurity; 3. To defend our nation from the many types of cyberwarfare tactics performed by America's adversaries. This initiative can best be started in the K-12 system.

Multiple stakeholders must be involved in order to develop the most impactful, institutionalized design possible; a design that impacts the most students while still allowing the individual classroom teacher freedom to be creative and adaptive. If this crisis is left solely to politicians, it may fail.

The following model is presented for discussion, debate, and open dialogue:

a. Establish regional teacher learning communities, sometimes referred to as professional learning communities. This is a recognized best practice that can both enhance teacher quality as well as empower teachers to lead. Teacher quality is the single most important factor when determining student success in the classroom. A teacher learning community (TLC) is not a staff meeting. Instead, a TLC focuses on collaboration, continuous improvement, and a growth mindset in

CSO Online: http://www.csoonline.com/article/2953258/it-careers/cybersecurity-jobmarket-figures-2015-to-2019-indicate-severe-workforce-shortage.html
Irish Times Online: https://www.irishtimes.com/news/education/the-myth-of-digital-natives-1.3459381

order to both teach the educator new skills as well as allow a place for dialogue. Within a TLC, teachers can share strategies and lessons that work as well as share items that do not work. This teacher-centered approach improves educator awareness and quality in order to benefit student learning. These TLCs also could create ideas for incorporating a standard based, multidisciplinary cybersecurity curriculum throughout the United States.

b. In order to be impactful, these TLCs will need a relationship with post-secondary academia and local cybersecurity experts. It is suggested that each TLC be led by at least one master teacher in each region. This master teacher would serve as a link between higher education, government/industry, and the K-12 environment as well as be responsible for leading established monthly professional development sessions on cybersecurity topics. The master teacher would need basic cybersecurity knowledge and serve to help others learn and adapt for individual disciplines.
c. All teachers will also need access to a shared online database or website to share and explore lesson plans. This website would allow interested teachers a "one stop shop" to explore lesson plans and activities for the K-12 classroom. Teachers would also be encouraged to adapt posted lessons and/or share new lesson plans to create the best resource possible. Contained within this website will be a cyber-ethics module for students in each grade band (grades 3-5; 6-8; 9-12). This ethics module could be used by all disciplines and all teachers in the K-12 classroom to instill necessary ethical guidelines.
d. After the establishment of the TLCs, a grant program could be established to bring longevity and a local approach to teaching cybersecurity within each school district. Under this proposal, interested school districts could apply for grant money to fund one cyber literacy outreach coordinator for the district. Responsibilities of this individual would mirror the established practice of utilizing instructional coaches within the K-12 setting. The cyber literacy outreach coordinator would "coach" individual classroom teachers in lesson development, hands-on activities, and co-teaching opportunities to both create new lessons and implement cybersecurity topics into current lessons. This person would also be responsible for attending professional development opportunities such as the

NICE K-12 conference to stay current and up to date on cybersecurity trends. The instructional coaching model has proven to be effective. Instructional coaches help teachers become better teachers by facilitating creativity and best practices. Better teaching methodology leads to higher student production.

e. Continuous in-person professional development should occur in the form of one-day cybersecurity boot camps that use the "teach the teacher" model. These events could occur in each region to begin the process of institutionalizing cybersecurity concepts into the classroom. The one-day boot camps would advertise to all teachers regardless of discipline or experience. A beginner session; along with an advanced session would be offered. Not only is there a desire amongst teachers who lack experience, but experienced technology/CS teachers strongly desire guidance in implementing cybersecurity into their coursework. Some teachers may not have the time or desire to commit to a TLC. However, completing a one-day session may encourage them to join the community.

The strategies described in this document are already being used; only the content topic has changed. Placing an increased emphasis on funding cybersecurity education initiatives in K-12, utilizing proven teacher development strategies, and establishing a community of multidisciplinary cybersecurity advocates within the K-12 setting will institutionalize the process of educating students on cybersecurity at a young age. These actions will solve the job shortage crisis, make Americans better cyber citizens, and prepare the nation for the ongoing struggles with foreign adversaries and bad actors.

Biography

Ms. Ashley Greeley received both her Bachelor's and Master's degrees from Purdue University. She began her teaching career in 2003. After two years in the special needs classroom, Ms. Greeley began teaching social studies at Harrison High School (West Lafayette, IN). While at Harrison, she developed two new courses for insertion into the curriculum (AP US history and AP US government), coached a variety of sports and an academic team, served as both department and corporation chair, led the school improvement team, facilitated teacher professional development, and served in whatever capacity asked of her. Greeley was awarded numerous teaching awards and recognition including the Golden Apple, the DAR History Teacher of the Year, the Indiana Historical Society Teacher of the Year, the Indiana History Teacher of the Year, the Indiana representative at the Supreme Court Summer Institute, and was a top-25 finalist for the Indiana Teacher of the Year Award. Beginning in 2015, Greeley began serving as a site visitor for GenCyber summer camps. In 2017, Ms. Greeley was awarded an NSA/CAE grant to develop a multidisciplinary K-12 cybersecurity curriculum as well as perform cybersecurity outreach for Tippecanoe School Corporation as an extension of the INSuRE program at Purdue University.

Meeting the Cyber Security Workforce Demand

By Drew Hamilton

Mississippi State University

Twenty years ago it was reasonable to think that the demand for computer security would crest as technological innovations secured what we now call cyberspace and our connection points into cyberspace. It was tempting to remember studies cited in the first information systems courses in the sixties showing curves that indicated that eventually every man, woman and child in the United States would need to become switchboard operators in order to meet projected demands. Of course that did not take place – technology replaced the vast majority of human telephone operators.

Currently, new technology is actually *increasing* cybersecurity workforce demands and broadening and deepening the skill sets required for the cybersecurity workforce – quite the reverse from the telephone operator issue. In this short paper, we will consider the following issues:

1. CyberCorps and its impact on the US Civil Service, the private sector and a revived DOD Information Assurance Scholarship Program (IASP)
2. Education versus training
3. New Technology and Cybersecurity education
4. Future Directions

1. CyberCorps and its Impact

The impact that the NSF CyberCorps program has had on the Federal cybersecurity workforce has been well-documented elsewhere. There has also been a positive impact on state, local and tribal governments. In many rural areas, the only way a state or local government entity can make a quality cybersecurity hire is with a Cybercorps graduate who has a service obligation and wants to stay close to home.

Early in the days of the SFS program, some PIs were encouraged to prioritize placements in non-DoD Federal Service. At that time, the DoD IASP was running a similar program, but one where student scholars were selected by the DoD agencies where they were expected to intern and then serve out their service obligations. But the DOD IASP did not consistently produce close to the number of scholarship students as SFS. With rumors of a revival of the DoD IASP, it may make sense for the DoD program to specialize in DoD-unique and mostly DoD-unique cybersecurity skills such as attack, exploitation and intelligence tradecraft.

While SFS has clearly impacted the Federal workforce, it has also had a major impact on the US private sector workforce. SFS enabled its Federal sponsors to "lock up" the best student talent early and commit them to government service. Industry has paid attention. Tech firms, particularly Tech giants Facebook, Amazon and Google are actively engaging with undergraduate students looking for talent with internships, co-ops and contract work during the semester. This is formidable competition because the tech giants have deeper pockets and fewer constraints then Federal agencies.

2. Education versus training

The critical shortage of cyber security workers has contributed to the rise of cyber security certification business. DODD 8140 (and its predecessor DODD 8570) ensures a government requirement that must be met. Additionally, non-defense industry also seems to favor graduates who have earned commercial cyber certifications such as Security+, CEH, CCNA-sec, etc.

Training, "the action of teaching a person or animal a particular skill or type of behavior" differs from education, "the process of receiving or giving systematic instruction." You can train someone to program in Ada and you can educate him/her in computer science to include programming skills. We train programmers in specific languages/environments and educate software engineers. Training is important, but tends to be of shorter-term value. Training strategies can

certainly be used as a stopgap measure to address critical personnel shortages. The Cybercorps program must remain focused on educating the cybersecurity workforce. Federal agencies may need to train new hires in specific skills Education is needed to provide the foundation for life long learning. Education on fundamental principals is the only way to "future proof" the education we can provide. Consider Coffman and Denning's 1973 classic *Operating Systems Theory*. It won't train a student on the Windows registry but the operating system design principles espoused in this work are still valid fifty years later.

3. New Technology and Cybersecurity education

University cyber security programs are challenged with having an increasing number of topics to cover. The NSA CAE Cyber Operations Program is an example of a specialized set of cyber security knowledge units that incorporate both current subjects as well as older fundamental subjects such as assembly language programming and reverse engineering as well as cyber operations tradecraft. The result is an academic program that is difficult to fit into a traditional degree program.

The NSA CAE-CO program is clearly geared to the production of cyber security scientists and engineers. While NSA is focused on the deeply technical side of cybersecurity, NSF CyberCorps meets a broader range of Federal government requirements including cyber security policy and information systems focused cyber security programs. An early lesson learned from the NSA CAE – CO effort is that it is very difficult to get deep coverage of all desirable cyber security skills in a single degree program. In NSA's case, there is also a need for its cyber security workforce to have specialized knowledge of intelligence tradecraft.

But the needs of the NSA are not necessarily representative of the entire Federal workforce. Different agencies have different cybersecurity workforce demands that are not all engineering based. Here is where the private sector needs differ from the public sector. Industry is demanding cybersecurity scientists and engineers and has much less demand for cyber policy and other "softer" cyber security skill sets.

New technologies are complicating this challenge. We are long way from having a single computer security course in a computer science program that was the norm fifteen years ago. Cyber security in software applications has expanded into other engineering disciplines and other colleges. Cyber security for SCADA systems, industrial control systems, IoT devices and High Performance Computing assets all require deep, specific technical knowledge that likely will lead to more and more specialized cyber security education and training programs. CyberCorps will receive applications from some of these newly formed, specialized programs and will need to consider whether these programs should become part of the SFS Scholarship program. This will further complicate the tradeoffs between technically and non-technically based CyberCorps educational programs. Should CyberCorps be cognizant that industry demands for cyber security professionals differs from government demands and plan accordingly?

4. Future Directions

ABET's recent move to accredit cybersecurity engineering academic programs is an important development. Future Cybercorps solicitations may wish to consider ABET accreditation in cybersecurity when evaluating new programs, particularly programs that do not fully meet the CAE criteria.

The author of "Dilbert," Scott Adams when asked, when asked if he had any advice for engineers, replied, "Engineers should work in organizations that value engineering." Having personally retired from Federal Service I doubted that government service would value engineers. However cyber technologies are rapidly changing that. NSA is clearly an organization that values engineers. Cyber technology is changing the Federal workspace and the security challenges are not only coming from amateurs and fraudsters, but also from nation state actors. While technology alone may not be sufficient to change attitudes in the Federal workspace, CyberCorps can and has. As more and more CyberCorps graduates rapidly advance

to leadership positions in the US Civil Service, they bring a new perspective to Federal cyber security that must continue to be nurtured.

Hamilton Bio-Sketch

Drew Hamilton is the Director of the Center for Cyber Innovation at Mississippi State University, a professor of computer science and engineering and leads the MSU NSF CyberCorps program. Previously he served as an Alumni Association Professor of Computer Science and Software Engineering at Auburn University where he initiated and led Auburn's SFS Program. He previously held faculty appointments at the US Military Academy and a visiting appointment at the US Naval Postgraduate School. Dr. Hamilton earned his doctorate in computer science from Texas A&M University. Dr. Hamilton is a distinguished graduate of the Naval War College

New Approaches to Cybersecurity Education Workshop

June 9-10, 2018, in New Orleans, LA

Proposal Submitted for the Steering Committee's Consideration

From Seth Hamman, Ph.D.

Author Academic Bio

Seth Hamman received the B.A. degree in religion from Duke University in 2002, the M.S. degree in computer science from Yale University in 2011, and the Ph.D. degree in computer science from the Air Force Institute of Technology in 2016. He is an Assistant Professor of computer science with the School of Engineering and Computer Science at Cedarville University. His research interests include improving cybersecurity education, and he has written journal articles and presented at national cybersecurity education conferences on the importance and practice of teaching adversarial thinking for cybersecurity. He has also been the recipient of two NSA National Cybersecurity Curriculum Program grants to develop curriculum for teaching adversarial thinking for cybersecurity and for teaching the legal and ethical aspects of cybersecurity.

Cybersecurity for All CS

The discipline of computer science is no longer in its infancy, but at only around 50 years of age, it is still in some ways in its adolescence. One of the next steps in its maturation must be for it to fully embrace security as a core part of its identity.

Because the benefits of "technology" (hereafter a catch-all term for the products of computer scientists) increase when they are networked together, the coming era of the Internet of Things is an inevitability. As this era comes about over the next decade, the distinction between technology and cyberspace will practically disappear. Therefore, securing cyberspace (i.e., cybersecurity) will be a concern of the vast majority of the next generation of computer scientists.

The movement of all technology into cyberspace is somewhat disconcerting because many of the properties intrinsic to cyberspace make it a fundamentally vulnerable domain. For example, cyberspace is *distanceless*, meaning that bad actors can operate at anytime from anywhere in the world, making the number of potential threat actors virtually limitless. Also, the world of cyberspace is *digital*, making it possible to perfectly impersonate others and trivial to steal, modify, and destroy cyberspace assets. Cyberspace is also *invisible*, cloaking nefarious activities in darkness. This makes it difficult to detect and to identify bad actors, enabling them to act with near impunity. These attributes (among others) combine to make cyberspace particularly susceptible to criminal wrongdoing, and history has shown that criminal bad actors are ready and willing to take advantage of these dynamics. These attributes also make cybersecurity, which is about protecting the rights of individuals and organizations in cyberspace, an enormously difficult undertaking.

Therefore, as cyberspace more and more becomes part of the core infrastructure of our society, all those involved in producing and deploying technology must be thoroughly security-conscious. Cybersecurity should be seen as a shared responsibility among all those involved in creating its artifacts and infrastructure. However, it is not clear that today's computer science programs are sufficiently emphasizing security to the extent that every graduate is security-minded. From my experience as a computer science faculty member and as a computer science graduate student over the past 10 years, security within the discipline of computer science is

still seen as something of a sub-discipline that some will focus on, while others are free to ignore. Again, this is especially disconcerting because increasingly, the proper functioning of our economy, the well-being of our citizenry, and the safe-guarding of our freedoms are all dependent on a secure cyberspace.

It is true that much progress has been made to raise awareness of this need within the discipline of computer science. For example, the CS Curricula 2013 guidelines made headlines for highlighting security as both a stand-alone and a cross-cutting concern. This was the first time in the history of the guidelines where security was specifically called out and represents a major step forward. However, the guidelines did not go far enough in emphasizing the importance of security. For example, the only time the word "security" is mentioned in the *Characteristics of Graduates* section, is under the *Familiarity with common themes and principles* sub-heading. The sub-section states, "Graduates need understanding of a number of recurring themes, such as abstraction, complexity, and evolutionary change, and a set of general principles, such as sharing a common resource, security, and concurrency." Again, it is good that security is mentioned in the context of characteristics of graduates, but the level of prominence assigned to it does not match its importance. In order to help create a more secure technological infrastructure, "security-minded" must be one of the foremost "characteristics of graduates."

Today we lament the fact that security concerns have frequently been an afterthought in the design, production, and deployment of technology, which has helped to lead us into an entrenched dependence on a vulnerable infrastructure. But with the current state of computer science education, these mistakes are likely to be reproduced by the creators of tomorrow's technology.

I recognize that this idea is not new. In fact, Eugene Spafford wrote about how computer security issues pervade every aspect of computing in the 90's in his testimony that in part inspired this upcoming NACE workshop. But I am arguing that to date, we (the cybersecurity education community) have not sufficiently prevailed upon our computer science colleagues to accept responsibility for incorporating security into their courses. This negligence has helped lead us into the present situation in the workforce where cybersecurity specialists

are continuously putting their fingers in a dike with new leaks sprouting around them all of the time. A continued push to raise awareness and ultimately to reorient the discipline of computer science around security is for me one of the most effective ways to deal the acute cybersecurity labor shortage.

Practical Next Steps

In order for computer science education to properly prepare the next generation of computing professionals, who are increasingly laying the groundwork for a technology-based society, the next stage in the maturation of computer science must focus on nurturing a security mindset in students. Producing a computer science graduate who is unconcerned with potential adversarial actions is like producing an accountant who does not appreciate the potential for an audit, or like producing a mechanical engineer who is not preoccupied with safety concerns. In short, it is irresponsible. Cyberspace is rife with threats, and no computer scientist should be enabled to remain ignorant of this fact.

I am not suggesting that cybersecurity should not be a specialized sub-discipline of computer science – it definitely needs to be, and I am sure that the NACE workshop will find ways to promote this from K-12 through graduate school education. I am also not arguing that every computer science graduate must be a cybersecurity specialist. But what I am suggesting is that every computer science graduate must be exposed to security concerns early in their course of study and throughout their program. It must be impressed upon every student that in addition to their expected user base, nefarious people exist with impure motives, and the threat they pose must be mitigated at every opportunity. We have done well at emphasizing reliability testing and the necessity for handling random natural events and unintentional human mistakes (which ported naturally from the discipline of engineering), but computer scientists must always consider potential adversarial actions as well (which is not a vital concern of most engineers).

We must work to promote cybersecurity among broad audiences of computer science educators. Already existing curricular guidelines like CS Curricula 2013 and CSEC2017 provide the specifics; our task must be making sure guidelines like these rise in prominence. One practical idea would be to push for security-related keynote addresses at future SIGCSE

conferences. Another idea is to work with ABET's Computing Accreditation Commission to better highlight and enforce security-mindedness as a student outcome. Teachers and faculty members reproduce what they are, and many of them are not security-minded, so another idea would be a to offer continuing education in the areas of cybersecurity for computer science teachers and faculty. Offering a free cyber workshop at major computer science conferences might be a great investment for equipping computer science faculty.

Preparing CyberSecurity Experts as Adjunct Faculty to Teach at the Post Secondary Level

Shelly Heller, Lance Hoffman and Costis Toregas
The George Washington University
Washington DC 20052

It is a well published concern that in order for the United States to maintain and expand its capabilities in the world of cybersecurity – whether planning new technologies and the internet of things (IoT), preparing defenses, constructing offensive tactics, or appropriate policies – a well-educated workforce is needed. To fill the numerous government jobs, many educational pathways have to be opened – including job training, community college programs and traditional four year and graduate programs. Each of these avenues educates and trains individuals to work at different levels and in different capacities in our 'cyber' world. Currently there is a capacity issue: students cannot readily be added to the education system, especially at the community college level, because trained faculty are scarce. The weak link in the cybersecurity workforce supply chain is often finding faculty who can be effective and provide the proper encouragement to students to join the cyber workforce. Therefore, success depends, in large part, on the capacity of our educational institutions to scale up and absorb increased numbers of students, as well as the capabilities of our educators.

The nation is looking to our community colleges as an untapped source of cybersecurity workers. According to the National Science Foundation, "Community colleges can play a critical role in giving students the hands-on skills that are needed on the front lines (of) defending computer networks[i]" According to the American Association of Community Colleges, there has been huge growth in the percentage of higher education faculty teaching in community colleges and the biggest group contributing to that growth are part time faculty. And, while some community colleges have existing programs in cybersecurity and have dedicated full time faculty, according to the Center for Community College Student Engagement, more than 58% of community college classes are taught by adjunct faculty. While the data is not broken out by discipline, an informal conversation with local community colleges is that they rely heavily on adjunct faculty, and many adjuncts may have no teaching experience. A typical advertisement for a cyber-security faculty member at a community college includes "Bachelor's degree (Master's preferred) and five years of work experience as Computer Forensics professional, technical qualifications: (CompTIA Network+, CompTIA Security+, CISCO certifications, CISSP, SANS, Certified Ethical Hacker (CEH)), knowledge of Programming Languages, excellent written and oral communications skills, experience in leadership including a history initiating and managing change, working with others toward shared goals and developing others." These

requirements can act as a barrier to many aspiring faculty members, thereby extending the mismatch between demand and supply.

Our answer: Tapping into cybersecurity experts as adjunct faculty. Cybersecurity experts in the workforce have the potential to fill the need for part-time cybersecurity faculty at the community college level. By tapping into the pool of working cyber security experts and retired individuals from government positions whose background fits the typical qualifications listed above, a viable long term strategy can be developed. These men and women, as government or private sector employees, often have had access to the latest technologies, wrestled with the current problems and policies facing the nation, have taken leadership roles and have a wide network upon which to rely for developing academic and career goals. In fact, they work with cybersecurity content on a daily basis.

Currently the Cybersecurity Teaching Corps project is exploring these possibilities through a research effort and a pilot "Teaching Cybersecurity at Community Colleges" online course (See Figure 1) funded by the U. S. Defense Department[ii]. While CyberCorps graduates generally possess the requisite cybersecurity content knowledge and experience to teach at a Community College level, they typically do not have teaching experience or knowledge of diverse learning and assessment techniques. Furthermore, most CyberCorps alumni are not a product of the community college pathway and they do not know the community college student and their unique challenges/opportunities. One can target the Cybersecurity Teaching Corps course to CyberCorps alumni with 3 to 5 years of work experience to address the typical requirements for adjunct faculty in community colleges or more broadly, to expand available adjunct faculty at four-year colleges and elsewhere.

introduction to Community Colleges, Ethics and general structure of a course
The typical Community College student, Faculty codes, Crafting goals and objectives
Teaching concepts – moving from concrete to abstract
Teaching concepts – using group work in your class
Teaching concepts – using case studies in your class
Teaching concepts – using discussions during a class

Figure 1: Cybersecurity Teaching Corps Course Content

[i] NSF (2013) Available on the web on December 8, 2016 https://www.nsf.gov/news/special_reports/science_nation/cybersecurity.jsp

DOD Grant: Grant# H98230-17-1-0371

NOVA | Northern Virginia Community College

April 30, 2018

Dear Sir/ Madam,

Here is a short submission for answering questions posted for this year's NACE Workshop. Due to seeing call of ideas late, I have only some ideas for consideration that I can expand should the committee want to hear more.

After teaching at George Mason University (GMU) and Northern Virginia Community College (NVCC) cyber and information assurance programs, students appear to lack the models and direction needed to develop into cyber professionals that have the foundations needed for success. Having a Model Activity Path (MAP) where students would see how the skills, classes, experiences link to actual work and needs in cybersecurity would make sense versus the traditional academic plans. Cybersecurity is truly a multifaceted domain that can be separated into areas such as policy, forensics, research, hardware, and other areas along with technical skills. Having MAPs developed by industry that features the skills and experiences employers foresee now and for the future would make the time, cost, and effort more relevant to students.

While many educational institutions have career paths and program curriculums, mapping those to actual work and careers is a challenge. As a hiring manager for a science and technology company, I have hired former GMU and NVCC graduates who perhaps use 20% of their education toward meeting client needs. As college is an exploratory along with development time for students, having MAPs developed along the lines of professional tracks would give students a visualization of where they can be upon matriculation. The MAPs would be developed through engaging industry to understand what is needed to "future-proof" the skills while helping educational institutions plan resources and classes. MAPs would also help level set the perceptions of cybersecurity toward reality versus fictional Hollywood versions of cybersecurity. For example, not all cybersecurity professionals are hacking or doing technical work.

An example of the MAP could be a Cyber Security Policy Analyst (CSPA). The MAP would encompass building skills in writing, legal research, sociology, and some technical courses. CSPAs would then help address the gap between the law and technology. Keeping MAPs current would show how the students could work toward real issues and adjust as companies seek new and current talents. MAPs would not be vocational nor prescriptive guarantee for job placement. However, the MAPs would show how the educational institutions are tuning the courses, content, and instructors to meet metrics for matriculations, rising stars with strategic companies for building institutional reputations, and doing relevant technical research.

My brief bio:

Published in IEEE and certified as a PMP, Mr. Hon proactively helps Federal clients with challenging projects and vendor management issues in Cyber Security, Cloud Computing, and Foreign Assistance areas for over 20 years. As a CISSP, Mr. Hon has also taught Cyber hacking and other technology courses for 17 years. He has spoken internationally and at numerous law enforcement

Thank you for your consideration!

Mun-Wai Hon, CISSP
MHon@nvcc.edu

Cybersecurity Education for Children of the Information Age

Cynthia Irvine

Naval Postgraduate School

April 2018

1. Problem Statement

A number of excellent programs have been developed to introduce K-12 students to cybersecurity. Examples include presentations by industry and academic experts; multi-day camps and gatherings featuring cybersecurity as a theme; and cybersecurity awareness days, weeks, or months that may involve discussions of cybersecurity and hands-on activities illustrating cybersecurity concepts and problems. Such activities can generate high levels of student interest in cybersecurity. They share two common characteristics.

First, these activities are discontinuous. Short intervals of high intensity learning may be followed by long periods during which student enthusiasm dwindles. Even with take-home materials, students may be set adrift. Without reinforcement, few students will progress between events. At the next event, students may be familiar with various topics but, with minimal advancement in the interim. To progress, students need practical tools for learning about cybersecurity, as well as help and encouragement from parents and teachers.

Second, short programs require the presence and deep involvement of cybersecurity experts. The paucity of such experts limits short programs in terms of their duration and participant numbers. Furthermore, there are far too few cybersecurity experts to provide on-location support to school districts nation-wide.

The relatively small number of students involved in short-duration programs is a serious issue. Mechanisms are needed so that substantially larger student populations have access to computing and cybersecurity education. These mechanisms must be formulated so that they can succeed in resource constrained contexts.

Parents can review the homework assignments and help children with reading, spelling, and standard arithmetic and mathematics. Similarly, teachers know how to present these materials in the classroom. Yet today, parents and educators are ill equipped to help children learn about computing and cybersecurity. Some may not even believe that these topics can be taught to their children.

Just as there are programs that encourage parents to read to their children, educational programs are needed to enable typical teachers and parents to help the children of the information age learn about computing and cybersecurity.

2. Idea: A Multi-pronged Approach

Public Appreciation

Greater public appreciation of the "wonders" of computing and cybersecurity is needed.

How can parents and teachers support their children and students if they know **nothing** about how computers work? They do know that computers are part of daily life. From smartphones to grocery store checkouts and utility meters, they know that computers are at work, but they don't know how. They may also be aware that cybersecurity is a problem. Yet most people have no idea of the true extent and vulnerability of the computing ecosystem. Cyberspace appears far too complicated and difficult to understand.

Why should this be so? Millions of non-scientists appreciate the wonders of the universe. They support space research and NASA programs. Similarly they appreciate the elegance of a well engineered car. They may know more about Stephen Hawking and concept cars than they do about how they are connected to their local ISP. Public education programs are needed so that citizens can appreciate the achievements and challenges associated with building and operating cyberspace. They can also be made aware of the opportunities and rewards associated with careers in cybersecurity. Such appreciation will not turn everyone into a computer or cybersecurity expert, but it will help parents, teachers, and others encourage young people to learn about and enter these fields.

An Environment for Ongoing Computing and Cybersecurity Education

To build and maintain student interest in computing, an environment that supports computing and cybersecurity tools and exercises should be available year-round. The environment should:

- Present low barriers to participation.
  - Be easy for typical teachers to use.
  - Its per-pupil cost must be low.

- Engage students and allow them to build and explore. It should be designed to encourage students to experiment and learn, not race to the finish.
- Allow students to progress at their own rate, while helping all students achieve a sense of self efficacy.
- Individualize student work. No copying from someone else!
- Allow disinterested students to quit (after mastering some minimum set of knowledge). Not everyone needs to play the clarinet, neither must everyone become a cybersecurity expert.
- Assist educators with routine grading tasks.
- Ensure that each student's performance and progress can be measured.
- Identify students needing assistance, and permit reenforcement of their basic knowledge and skills before moving them to more difficult concepts and tasks.
- Allow parents to appreciate student progress (see below).

Objectives for the overall environment might include:

- Respect privacy.
- Support statistical analysis of ongoing results. For example, it may be desirable to understand how the environment works for different social and economic populations.
- Design for rapid extension and adaptation. It should be possible to roll out new versions of the tools relatively quickly.
- Allow alignment with the cognitive development of students. Measures of student readiness in terms of information processing, abstract reasoning, etc. for certain topics would be useful. This would prevent frustration for for both rapid and evolving learners.
- Reward persistence, not competition.

Ultimately, high aptitude students can be identified and encouraged to pursue advanced cybersecurity studies. Students with other goals will benefit from an appreciation of how computing and cybersecurity work and will be better cyberspace citizens.

Companion Tools for Parents and Educators

Easy to use tools should be developed to allow parents and teachers new to computing and cybersecurity to support and follow student progress. Student homework tasks should be designed so that parents can know that children are completing their assignments, despite not understanding the details of those assignments. However, it should be possible for parents to learn along with their children. Individualization of assignments can ensure that parents-as-learners are not doing their children's homework for them. Similarly, tools can be constructed so that teachers could learn along with their students.

A benefit to having parents and teachers learn in parallel with students is that some may find that they have the aptitude and proficiency to pursue professions in computing and cybersecurity. If structured properly, these individuals could continue their studies in post-secondary education programs.

Use Cybersecurity Experts Wisely

Computing and cybersecurity experts will be needed in all facets of this effort. Public appreciation of cyberspace and cybersecurity will require translation of technical topics to the general public. Everyone needs to have some understanding of how cyberspace intersects with and affects the physical world. Lessons and tools will need to be designed to cover not only how computers and cyberspace constructs are built and operate, but to address a plethora of social, legal and ethical issues. Mechanisms to ask for and receive help with aspects of the environment will needed.

Closing Note

Although this paper focuses on K-12 students, many of the concepts associated with the proposed environment could be applied to post-secondary education in cybersecurity, both traditional or nontraditional.

New Approaches to Cyber Education (NACE) Workshop

Educate the Educators to Equip the Next Generation

By: Joni L. Jones Associate Professor Information Systems and Decision Sciences, Muma College of Business, University of South Florida

When considering the education needed to equip the next generation to become cybersecurity and privacy specialist we need to address who to educate, what to teach, and how to sustain the pipeline. Cybersecurity is a rapidly evolving arena of topics and mindsets. We need to concentrate our efforts in creating students that can think and react to this environment. In order to make our efforts fruitful we need to start in K-12 where we have the largest potential candidate pool and most malleable minds. Two main focuses are a basic understanding of technological topics. Essential core technology skills include programming and computer literacy, networking and internet connectivity, big data/data privacy and ethical issues exacerbated by the ubiquitous nature of technology. More importantly, students need to be comfortable with experimentation and experiential learning. In this fast paced milieu students and eventual practitioners must be self-motivated problem solvers that question norms, propose inventive solutions and out think the cybercriminal. As university academics we need to focus our efforts on preparing instructors with the necessary skills to make this happen. Our focus should be on training the trainers.

The question then becomes how do we create such students? Much of our current education is based on route memorization and lecture. Moving toward a more experiential learning experience is imperative to engender the skills needed for successful cybersecurity and privacy specialists. Therefore, the first task should be to educate the educators. According to the State of the States Report: State-Level Policies Supporting Equitable K-12 Computer Science Education (2017) "There are simply not enough adequately trained people to full the current need for information security analysts, hardware engineers, software developers, computer programmers, data scientists, and other STEM professionals (pg. 7, Stanton, et al. 2017)." For example, according to Code.org, only 241 schools in FL (22% of FL schools with AP programs) offered an AP Computer Science course in 2016-2017 (13% offered AP CS A and 16% offered AP CSP), which is 95 more than the previous year. There are fewer AP exams taken in computer

science than in any other STEM subject area. Additionally, Florida universities did not graduate a single new teacher prepared to teach computer science in 2016. This deficit indicates an area where assistance is needed in the form of tools and experiential learning materials and environments that are easily deployed by all faculty. These experiential learning materials could include project or game based lessons such as capture the flag, hackathon, or team competitions. Cyber ranges and other technical playgrounds are essential to facilitate these type of experiences in contained and safe settings. With these type of educational tools you are also advancing problem solving skill building. Organizations similar to DECA (Distributed Education Clubs of America) and the Whitehatters should be recruited to develop and hold national competitions to act as a resource, outlet, and incentive.

Another major motivator to attract and educate a diverse set of students to succeed in a variety of national and private sector positions is to ensure that students know the career paths an opportunities available to them. Increasing the visibility of positions, the skills required, salary ranges, daily activities, etc. will allow students to visualize themselves in the career path and drive enrollments. Not every student may choose a traditional 4-year university degree so there needs to be a variety of paths to acquire the necessary skills. These paths could include vocational training, community college, as well as the traditional 4 year university degree. All should employ High Impact Practices (HIP), namely, internship opportunities to gain hands on experience. Unfortunately, in the area of cybersecurity this can be difficult due to security issues with organizations. Alternatively, other HIP experiences could include case based learning, capstone courses or other settings that pose situational conditions to students that require problem solving and an opportunity to apply their learning via a culminating assignment.

To ensure that the education we provide is consistent and executable requires a concerted centralized structure of support. A centralized body would need to be responsible for establishing standards and curricula, promoting best practices, providing continuing education, and accreditation. They can also participate in the creation and hosting of national and international competitions and/or establish a national student organization.

While cybersecurity education cannot be expected to train for every platform it is imperative that academia and industry form partnerships. These partnerships should include externships for faculty to work with industry to develop curriculum and gain valuable field experience. To enable hands on training industry can collaborate with higher education to create environments, cyber ranges and other training materials to enhance student engagement and practical skill development. Corporations and cyber application developers are uniquely positioned to supply expertise and fund/donate technology. Academia can then generate, possibly in partnership with industry, lessons and curricula that utilizes the corporate supplied technology and use cases.

In summary, to ensure that we keep pace with the ever-changing and rapidly growing need for a cyber-ready workforce we need to work collaboratively with K-12, industry, and upper level academia. This public-private partnership will blend classroom learning with workplace experiences. We need to train the trainers on technologies and cyber trends to facilitate this learning. More importantly, we need to expand and facilitate experiential learning to promote student's problem solving skills, encourage persistence and integrate their knowledge into a contextualized experiences.

References

Stanton, J., et al. 2017, State of the States Report: State-Level Policies Supporting Equitable K-12 Computer Science Education (2017) Retrieved from http://www.edc.org/sites/default/files/uploads/State-States-Landscape-Report.pdf

Schaffhauser, D. (2017) State Progress on K-12 Computer Science Ed Policies: 'We Have a Long Way to Go' *THE Journal – Transforming Education through Technology (04/10/2017)* Retrieved from https://thejournal.com/articles/2017/04/10/state-progress-on-k12-computer-science-ed-policies.aspx

K12 Computer Science Framework (2016). Retrieved from http://www.k12cs.org

BIO

Joni Jones is an Associate Professor in the Information Systems Decision Sciences Department and Academic Liaison for the MS Cybersecurity Degree Prohgrams. She teaches various graduate and undergraduate courses including global cyber ethics, decision analysis for business

continuity and disaster recovery, systems analysis and design, business honors professional development, and research methods. She previously taught introductory courses in computing as well as courses in C#, managerial statistics, business system application and design, and software applications.

Her research interests include electronic commerce, pricing models for information goods, information and prediction markets, social networking and cyber ethics. Her research has been published in the MIS Quarterly, Production and Operations Management, the Journal of E-Commerce, INFORMS Journal on Computing, Decision Support Systems and presented at national and international conferences.

Jones holds a BS in business administration from the University of Illinois, Chicago, and earned a PhD from the University of Florida. She joined USF in 2003, having previously taught at the University of Michigan, the University of Florida, and Santa Fe Community College. Her professional service includes roles as a reviewer for numerous academic journals. She is a member of Beta Gamma Sigma.

A Cyber Security Library – The need, the distinctions, and some open questions

Sidd Kaza, Department of Computer and Information Sciences, Towson University,
skaza@towson.edu

It is clear that in order to address the cybersecurity education and workforce crisis, the challenges are not just numerous but also inextricably linked. The least of which include a greater number of prepared faculty, effective curriculum, and infrastructure to host, use, and disseminate the curriculum. There is a demonstrated need for a cybersecurity digital library (DL) that will help address these challenges. The Cyber DL is similar to other curricular digital libraries in some respects (material quality, uptake, etc.) and unique in others (national security concerns, presence of damaging material – malware, material integrity issues, etc.). This idea paper articulates the need, the similarities, the distinctions and open questions, and provides some insights based on an ongoing Cyber DL project.

A Cybersecurity Digital Library – The need

Perhaps the greatest challenge to a successful digital library is the buy-in of the community behind it. For a cybersecurity digital library, this community includes academicians, industry, government standards and designation bodies, and the students who need the effective curriculum to contribute to our nation's workforce. Academia has taken advantage of the funding available from the National Science Foundation, National Security Agency, Department of Homeland Security, and other funding agencies available in the cybersecurity education arena. We have clearly reached a tipping point where there is effective curriculum to be had, only if there was a place to find it. There are early innovators responding to the need for curriculum sharing in cybersecurity education, such as CyberWatch, Department of Homeland Security (DHS), and SkillsCommons.org. There are similar efforts in computer science such as Ensemble, EngageCSEdu, NCWIT and in other STEM fields as well. The existing repositories offer several good features and a solid base on which to build, but there are several issues that need to be considered in the five-year horizon for a cybersecurity digital library to succeed.

A Cybersecurity Digital Library – learning from others

Vannevar Bush suggested the use of computers to retrieve information in 1945 (Bush 1945). The most recent surge in the term "digital library" came with the National Science Foundation funding research in the area through the Digital Library Initiatives through the nineties and into this century. There is a much cited formal framework focused on Streams, Structures, Spaces, Scenarios, and Societies to define digital libraries rigorously (Gonçalves et al. 2004) - Streams are sequences of items that describe static and dynamic library content. Structures are labeled directed graphs, that impose organization. Spaces are sets with set operations that obey certain constraints. Scenarios consist of sequences of events that modify states of a computation in order to accomplish a functional requirement. Societies are sets of entities and activities and the relationships among them.

A successful Cybersecurity Digital Library effort, has much to learn from the DL literature on what makes a "good digital library." There can be several quality indicators of the digital objects, metadata, collections, catalog, and services for a digital library. These include (Goncalves et al. 2007) accessibility, accuracy, completeness, composability, conformance, consistency, effectiveness, efficiency, extensibility, pertinence, preservability, relevance, reliability, reusability, significance, similarity, and timeliness. This is a rather long laundry list of quality indicators, and each is accompanied by metrics to measure them. As we build a Cyber DL, we will need to interpret and apply each of these to the new digital library.

A Cybersecurity Digital Library – Distinctions

There are several unique aspects and challenges to a Cyber DL that have not been explored in the digital library literature. In our work in building a prototype Cyber DL (www.clark.center) and working with the community, and beta-testers, we have identified the following issues (technical, policy, and social) that highlight the distinctions.

Complicated security policies – A Cyber DL will likely store cybersecurity curriculum that might provide the knowledge needed to cause malicious damage. One might argue, that such

knowledge is found quite easily at other places on the web. However, this curriculum might be accompanied by pieces of Malware that will be used in sandboxed environments in the classroom (a rather common practice in security courses). Security policies need to be implemented to host, distribute, and sandbox this Malware. How do we ensure that an open Cyber DL does not become a "Dropbox" for Malware? How do we ensure that only qualified faculty have access to the materials?

Disclaimers and protection – Closely related with the previous policy issue, is the protection that a Cyber DL will need to have from potential damage the distributed content might cause. Does there need to be protection for the host – whether it be a university, a non-profit, or a private company?

Attacks from adversaries – As with any large-scale web application, security and availability would be a concern for the Cyber DL. However, producing cybersecurity professionals also contributes to our national security. Would a national Cyber DL become a soft target, needlessly attracting attention as it hosts curriculum that our CAE and other institutions use? If this indeed is an issue, what protocols and resources need to be in place to mitigate this risk and are they any different from other digital libraries?

Faculty incentives – Cybersecurity curriculum is challenging to build, deploy, and update. Though other disciplines might be similar, we can contend that cybersecurity learning materials will need to be updated more frequently and will require a dissemination plan so content consumers are not just notified but also involved in the maintenance of materials. If that is the case, the Cyber DL needs to include an incentive plan for content creators. Maybe a music subscription like plan ("the artist gets a small cut for each download") or maybe a 'tipping' system (recommended at a recent workshop). In the age of Kickstarter, is a crowdsourced sustained funding source the way to go?

Storage, licensing, and dissemination – Several cybersecurity materials come with virtual machine (VM) environments that cater to the learning objects. Even with the seemingly endless storage capacity and bandwidth that we appear to have available, distributing VMs becomes a problem that scales very quickly. Cyber DL solutions will need to look at creative ways to not just store, but create a versioning for VM images, look at software licensing issues (and not become a "Dropbox" for pirated software), and look at bandwidth scaling very carefully so frivolous multiple downloads do not lead to escalating hosting costs. Should the Cyber DL consider partnering with a Cyber Range (Dark et al., n.d.) or maybe partner with a corporation (like Google) to donate storage and bandwidth?

The challenges in building a Cyber DL are many, but a discussion to answer some open questions will go a long way in making this digital library successful.

Acknowledgements

At Towson University, we are working on a pilot for a Cybersecurity Digital Library called CLARK (Cybersecurity Labs and Resources Knowledge-base, www.clark.center). CLARK is supported by the National Security Agency under NSA Grant H9830-17-1-0405. Though the language in this idea paper is the author's, some of the ideas are shared with Melissa Dark and Blair Taylor in their capacities with the NSA College of Cyber. To remove conflict of interest, neither Dark or Taylor reviewed this paper prior to submission.

References

Bush, V. 1945. “As We May Think.” *The Atlantic Monthly*, 1945.

Dark, M., S. Kaza, S. LaFountain, and Blair Taylor. n.d. “The Cyber Cube: A Multifaceted Approach for a Living Cybersecurity Curriculum Library.” In *The Colloquium for Information Systems Security Education (CISSE)*. New Orleans, LA.

Gonçalves, Marcos André, Edward A. Fox, Layne T. Watson, and Neill A. Kipp. 2004. “Streams, Structures, Spaces, Scenarios, Societies (5s).” *ACM Transactions on Information Systems* 22 (2). ACM: 270–312. https://doi.org/10.1145/984321.984325.

Goncalves, Marcos Andre, Barbara L Moreira, Edward A Fox, and Layne T Watson. 2007. “‘What Is a Good Digital Library?’ A Quality Model for Digital Libraries.” *Information Processing & Management* 43 (5): 1416–37. https://doi.org/10.1016/j.ipm.2006.11.010.

Author Bio

Dr. Sidd Kaza is the Chairperson and Associate Professor in the Computer and Information Sciences department at Towson University. He received his Ph.D. degree in Management Information Systems from the University of Arizona. His interests lie in cybersecurity education, data mining, and application development and he is a principal investigator on several cybersecurity education projects. He is also on the ACM Joint Task Force on Cybersecurity Education and is the recipient of the University System of Maryland Regent's Award for Excellent in Teaching. Dr. Kaza's work has been published in top-tier journals and has been funded by the National Science Foundation, National Security Agency, Department of Defense, Intel, and the Maryland Higher Education Commission.

New Approaches to Cybersecurity Education: CTF 101 Elective

Rana Khalil
University of Ottawa
https://rkhal101.github.io/

1. Introduction

Despite being one of the fastest growing fields, it is estimated that there will be 3.5 million unfilled cybersecurity positions by 2021 according to a recent report by Cybersecurity Ventures [1]. The reasons behind this cybersecurity labour crises are many, however one of the significant contributing factors is the lack of cybersecurity knowledge and skills. Individuals who obtain their degrees in areas such as computer science have a weak foundation in security principals. The approach used to introduce students to computer security usually involves either only introducing security in upper level courses or integrating security into the curriculum by quickly brushing over the theory behind the related security concepts with little to no practical exercises. In both cases, the students of such institutions graduate without a solid foundation in the basic computer security concepts. Introducing security across the curriculum through practical exercises is not a new concept and has been suggested by academia over and over again [2] [3]. Although the approach taken by institutions to implement this change has been lacking and many improvements can be suggested, this is not the focus of this proposal.

This proposal is inspired by an elective mathematics course implemented by the University of Ottawa in order to introduce students to the field of statistics and probability. The course is called Poker 101 [4] and was introduced as a creative way to teach students across all faculties about core concepts in probability and statistics. The course was first offered in 2011, and although it was offered as an elective, students from several faculties registered and successfully completed the course [5]. Using this innovative approach to teach probability and statistics, this proposal suggests the implementation of a course teaching the core concepts of computer security using the methods in capture the flag security competitions.

2. Capture the Flag 101 Course

The idea is simple. Capture the flag security competitions are known to be attended by individuals from diverse academic backgrounds. Due to the lack of security education in non-cybersecurity degrees such as computer science and software engineering, these individuals are also usually self-taught. However, due to the nature of capture the flag competitions where participants are given exercises to complete with little to no information or prior training on how to approach these exercises, many promising individuals might shy away from participating in such competitions, especially individuals that belong to minority groups. As a result, such individuals miss out on a great opportunity to learn and practice the security skills that the industry is in desperate need of.

This report proposes the implementation of an elective course that teaches the core concepts and skill sets required to participate and complete capture the flag competitions. This would include topics such as forensics, cryptography, web exploitation, reverse engineering and binary exploitation. The concepts would be introduced and taught to the students with the tools necessary to understand these concepts. Then students are presented with challenges to apply these concepts.

An implementation of such a course, especially at an early stage of a degree, will inspire students to pursue a career in cybersecurity or at the very least compel these students to be more security aware when taking other courses in their degrees. Another direct benefit of such a course is that students will be more encouraged to participate in CTF competitions and therefore further their skill set.

3. Conclusion

This report proposes the implementation on an elective course that teaches the core computer security concepts in the style of a capture the flag competition. This was inspired by a successful mathematics course introduced by the University of Ottawa, called Poker 101, that introduced the core concepts in the field of probability and statistics. Offering such a course can inspire students to pursue a career in cybersecurity and make students more security aware in the degrees they pursue. Implementation of such a course is very feasible and is likely to be successful considering the significant interest in CTF competitions from individuals pursuing both cybersecurity and non-cybersecurity degrees.

References

[1] Cybersecurity Jobs Report 2018-2021. https://cybersecurityventures.com/jobs/, Last accessed: 2018-04-30.

[2] Major Gregory White. Security across the Curriculum: Using Computer Security to Teach Computer Science Principles. 1996.

[3] W. Dwayne Collins. Introducing Computer Security Concepts in Introductory Computer Science Courses. J. Comput. Sci. Coll., 20(6):41–47, June 2005.

[4] Probability and Games of Chance! Poker 101. http://mysite.science.uottawa.ca/phofstra/MAT1374/index.html, Last accessed: 2018-04-30.

[5] Using math to beat the odds. https://www.uottawa.ca/gazette/en/news/usingmathbeatodds, Last accessed: 2018-04-30.

Author's Biography

Rana obtained her Bachelor of Computer Science and Mathematics at the University of Ottawa and is currently pursuing her Master of Computer Science with a focus on open source web application vulnerability scanners. During her time at university, Rana took upon herself various volunteer and leadership roles which included University of Ottawa ambassador for Seeds for the Future Huawei Canada, Orphan Sponsorship Initiative Vice Chair, Women Startup Network Peer Mentor, IEEE University of Ottawa Student Branch VP Academic and IEEE University of Ottawa Student Branch Women in Engineering Vice Chair.

Rana has worn many hats during her work in the public and private sector. She held positions as a spectrum engineer assistant, automated tester, software developer, security analyst and as a ransomware researcher. Rana currently works at the University of Ottawa as a Teaching Assistant for several second and third year Computer Science courses. As a teaching assistant, Rana teaches weekly lab/tutorial sessions, holds weekly office hours, marks theory and programming assignments and proctors midterms and final exams.

Rana is deeply passionate about her degree in computer science with a deep interest in computer security and is determined to make a difference using the degree she is pursuing.

Integrating Ethics in Cybersecurity Education

Mohammad Taha Khan, Chris Kanich and Cynthia Taylor
University of Illinois at Chicago and Oberlin College
{mkhan228, ckanich}@uic.edu, cynthia.taylor@oberlin.edu

Introduction

Ethics plays a critical role in cybersecurity and provides the moral distinction between black-hat hackers and cybersecurity professionals. The study of ethics in cybersecurity is a complex matter, and as the need for security professionals grows, educators and employers alike have focused more on raw numbers and technical competency than on ensuring that these professionals understand the ethical underpinnings of their sensitive and important roles within any given organization. Whether dealing with entrusted personal user data, developing a framework to store passwords, or investigating a data breach, all such tasks must be executed ethically which requires training beyond the technical aspects of cybersecurity.

Ethics has long been considered important to Computer Science in general, with the ACM and IEEE model curriculums both including it, and ABET requiring coverage of ethics for accreditation. In 2006 Quinn [1] showed that fifty-five percent of ABET accredited CS departments teach computer science students about ethics through a dedicated course on the social and ethical implications of computing, and argued for the benefits of offering ethics courses taught by Computer Science professors. As cybersecurity itself becomes a highly specialized and in-demand branch of computer science, its adversarial, mission critical role coupled with stewardship over an organization's critical infrastructure and private data necessitates a more specialized ethics curriculum tightly integrated into security-related courses.

Here we outline how to improve the overall instruction of computer science ethics by refining the content of the sole ethics course offered for computer science majors and by

integrating ethics into computer science courses. In addition, we suggest pointers which can be useful in training students from diverse backgrounds for practical situations.

We believe that teaching ethics as an integral component of cybersecurity education will empower future individuals to act responsibly when dealing with sensitive data. These suggestions will also help them better understand the irreversible implications of data breaches and hence promote the adoption of more secure and correct programming practices. Finally, a part of this ethics training, students will also learn how to carry out due diligence in situations of cyber attacks and breaches. The next sections provides details of our proposed ideas.

Suggested Approaches

Teaching The Ethics of Privacy Through Personalized Experiences: Ethics and privacy go hand in hand and a lot of components of ethics for cybersecurity revolve around safeguarding privacy. While the notion of privacy is extensively covered in the traditional computer science ethics course, the descriptions and examples can sometimes be too broad and hence result in a disconnect of the students understanding of privacy in context and it can be hard for individuals to understand the gravity of personal information leakage. However, all college students have personal experience with making their own data available in varying degrees online. By having students take surveys on how they currently share data or discuss the ramifications of having their data made public in various hypothetical situations, instructors can explain the ramifications of privacy policies in a realistic, student-centered way. It is also important that instructors discuss that the ramifications of data becoming public will vary greatly depending on the individual: for example, past dating profiles becoming public may have a very different implication for someone who is gay than for someone who is straight. These activities need to be designed in a meticulous and fine grained manner and require the involvement and overlapping interaction of ethicists and cyber security professionals to sketch out an accurate design.

Including Ethics Components Within Cybersecurity Courses: When ethics is included in the CS curriculum, it is usually taught as a separate course. Even when it is a required course for graduation, it is frequently seen by students as an "easy A" course, and less important than more technical courses. This, combined with the abstract nature of the course frequently results in students not taking much interest, and failing to develop the full practical context of ethics and its importance. Given the importance of ethics to cybersecurity, it's important to add ethics to security courses themselves, as well as covering cybersecurity topics in general ethics courses. This should be done by the including both case studies as well as collaborative exercises. Students should be provided case study readings that pertain to the technical material being covered in class. For instance, while teaching them about SSL and secure web applications, students should have readings about how the Heartbleed bug was committed to the OpenSSL and how it went undetected for years and had catastrophic implications.

Another example of having a more involved activity on ethics can be having students perform an SQL injection (as a part of their assignment) on a sample healthcare database. For submitting solutions, apart from providing malformed queries, students should be asked about their perceptions on how they felt about the data leaked and what possible implications it could have. This will not only allow them to learn the importance of dealing with sensitive data but also provide implicit feedback to the instructor to better evaluate the understanding and perceptions of ethics.

This supplementary approach to teaching ethics will not only strengthen the principles of the students, but will also provide them with real-world examples and implications, which will encourage better programming practices and enable them to realize how as cybersecurity professionals, their design decisions can impact millions of individuals.

Acquiring Industry Feedback: Finally, we also suggest that gaining feedback from senior level cyber security professionals can also helpful and can help develop a more practical curriculum. This can be done in the form of meetings, surveys as well as workshop or panel based interaction where educators can get real insights on what are

the main elements and components of ethics that should be focused on within the courses.

Ethics Within Graduate Security Courses: While the major proposed focus of this idea paper revolves around improving the ethical standards of undergraduate cybersecurity courses, at the same time, it's an important to realize that there should also be continued ethical training for graduate students. This is especially important as students without a US-based undergraduate education are less likely to have been exposed to ethics courses as part of their undergraduate education. Just as students are exposed to more complex computer science problems as graduate students, they should likewise be exposed to more complex and nuanced ethical issues.

Conclusion

Overall, we believe that a more integrated ethical framework is the right step forward in the direction of educating the cybersecurity professionals of tomorrow and will likely avoid situations like the Target breach or Cambridge Analytica. It is our hope that coupling ethics with mainstream technical education will result in better trained cybersecurity professionals.

References

[1] Quinn, Michael J. "On teaching computer ethics within a computer science department." Science and Engineering Ethics 12.2 (2006): 335-343.

Authors Bio

Mohammad Taha Khan is a 4th year PhD student at the University of Illinois at Chicago. His research interests span the domain of security and privacy on the Internet. His focus is on understanding privacy leakage on the Internet, socio-technical aspects of cybercrime and human factors in security. As a lot of his work incorporates insights from empirical analysis, he is particularly interested in developing better teaching methodologies around the ethics of data collection and management. After graduation, Taha plans to pursue teaching based academia.

Chris Kanich is an Assistant Professor at the University of Illinois at Chicago. He conducts research on the socio-technical aspects of cybersecurity. His current work includes analysis of gains and losses due to undesirable activity on the Internet, investigating human factors in effective Internet security mechanisms, and building new technological primitives with the goal of increasing the practical security and privacy of Internet users.

Cynthia Taylor is an Assistant Professor at Oberlin College. Her research interests include Security and Computer Science Education. Her education research interests include active learning, with a focus on peer instruction, and assessment of student learning via concept inventories. Her security research looks at how people use the internet, and its implications for security.

Denise Kinsey

Submission #1 nace@cerias.purdue.edu

Proposal paper in support of 'shared' cybersecurity special topics course.

While it supports many of the ideas presented in the CFP, this paper offers an approach that specifically addresses these questions:

- What skills and knowledge should people in the field have, and how should that be acquired?
- How do we get more US citizens—and a more diverse population —into cybersecurity in meaningful ways?
- What kinds of resources and materials for use in education and training are needed, how do we get them developed, and how do we measure their effectiveness?
- What are some good ways to "future-proof" the education we provide?

One issue plaguing academia is the need for timely information and training yet by the time a 'new' or cutting edge course is created it is outdated and in need of a refresh. While adding current events helps it does not address the fact that faculty can't be experts in everything or hold experience and credentials to teach every topic encompassed in 'cybersecurity', which means each term only a select few are fortunate enough to attend classes by experts in cybersecurity niche topic areas.

I propose that an emerging technology course is created, but instead of teaching or training a few teachers how to replicate the material, which is quickly outdated and for which they may not hold the necessary expertise, that the program recognize the experts in those areas and synergize the classroom by offering that special topic course on emerging technologies to other schools at the same time through a webcast format. Attendees would need the same level of pre-requisite skills, but this proposal extends teaching specialty topics to a few faculty to instead teaching many classes across the country at the same time each semester.

This proposal allows for recognition of cybersecurity experts while extending the reach of their expertise from a handful of teachers to many students across the country (or online if deployed military, etc) to allow them to gain knowledge in these emerging or niche topic areas where we have a pronounced need. It eliminates the need for schools to be seen as competitors and instead as compliments as competing programs and duplication of expensive resource labs may become a thing of the past.

How would such a proposal work? The teacher of record at each school is still responsible for their class in whatever format it is offered. The web hosted teacher can do this in conjunction with teaching their own classes of the same topic at the same time. The teacher presenting the material (web host/remote teacher) would create some resources for the remote on- ground faculty including a detailed rubric for each assignment, prerequisite readings, etc. to ensure that the students watching at a distance have the ability to understand the material and their teacher has the information to properly score the assessments.

The class would be taught by a combination with the expert in a web-format/webinar so the expert may broadcast from their home school/lab and all participating schools may benefit. This highlights the expert and allows all to benefit from that expertise, and it allows for schools to specialize in certain areas while still offering additional electives and specializations that otherwise would not be options for that student population. To accomplish this, the expert teacher who broadcasts the material will receive an additional stipend and the teacher of record from participating schools will still be paid as the local teacher as this person needs to grade, interact, answer questions, and facilitate the learning process. This type of cross-school and cross-class partnership has many benefits as all who participate are paid, the skills of the expert are shared to a broader audience, it reduces unnecessary or inferior replication of course topics, offers an audience to non-traditional applications or specializations in cybersecurity, and extends the reach of necessary course content beyond traditional classroom borders.

The webinar should be an interactive session allowing the on-ground faculty in each class to gather questions and assist their class. The on-ground teacher can augment the material with

additional items to aid in understanding or make it more relevant to the participating population. These items can include current events, grading course projects and research, guest speakers from industry and government, application of how the content applies to cybersecurity compliance, regulation, and governance.

The teacher hosting the webcast class would receive a stipend for the course materials and remotely teaching the sessions (for all class periods or a pre-determined number of times within a course to demonstrate the most difficult topics or concepts the remote school can't supply (such as those needing a specific lab set-up to allow for successful demonstration)), and for assisting local faculty in teaching and challenging their population of students.

The web portion should not be used as a recording to replace teachers, but should only be used in the event of class cancellation, to facilitate review in remote areas (such as military students deployed in drastically different time zones which would prohibit real-time attendance at the webcast, or daytime courses when the expert only teaches in the evenings for example) or to allow for review and remediation of the material. To keep the content fresh and to compensate the remote teacher for their effort and expertise, live webcasts should be performed.

This proposal addresses the need for flexibility in cybersecurity curriculum to address emerging topic areas, matching newer faculty or those untrained or lacking experience in an area of cybersecurity which is essential to student success in the workforce, and removes the financial barrier to many schools offering timely and necessary cybersecurity subjects, while showcasing the excellence held by some institutions in various cybersecurity areas. This is a concept that would require trust by both schools and the involved faculty, but which may ultimately solve some of the issues faced by our present lack of capacity to meet the needs of business and industry, resulting in our shortage of well-trained and educated cybersecurity workforce. Opening up the expertise in some of the topic areas may inspire greater enrollment by women and minorities as they would have access to these niche classes at their local college. It also offers the opportunity to showcase experts who may be women and minorities to areas of the country that have a less diverse faculty. Finally, this concept meets the CAE/CAE2Y requirement of shared teaching and resources.

The created material would become part of the collection made available to the CAE community – maybe hosted by CyberWatch or CSSIA in their curriculum repositories for designated schools to use. This could be limited to CAE/CAE2Y schools as a means of validating the pre-requisite and foundational skills and as an added benefit of becoming a CAE.

Denise Kinsey

Submission #2 nace@cerias.purdue.edu

Proposal paper in support of uniquely crafted externships/course projects.

As with proposal paper #1, this proposal supports many of the ideas presented in the CFP and specifically addresses these questions:

- What skills and knowledge should people in the field have, and how should that be acquired?
- How do we get more US citizens—and a more diverse population —into cybersecurity in meaningful ways?
- What kinds of resources and materials for use in education and training are needed, how do we get them developed, and how do we measure their effectiveness?
- What are some good ways to "future-proof" the education we provide?

One area lacking significantly in cybersecurity education is hands-on experience that aids in student learning and which can be listed on student resumes. In academia, most learning is passive which makes recall and complete understanding of a subject more difficult. This results in a shortage of well-educated and trained workers in cybersecurity. Students learn best and have a means to 'relive' the experiences through relevant, hands-on learning. One way to help students understand the cybersecurity job environment, and therefore provide a better assessment of understanding than traditional lecture courses, is to provide an immersive experience through in-depth, real world projects. Presently, most cybersecurity topics are presented as silos and not infused into other disciplines or even shown as a compliment to other IT and cybersecurity content areas. Learning requires context and a base of knowledge to best apply those concepts to situations, resulting in students synthesizing ideas to create solutions, just like what is expected when students are on the job.

To solve this problem we could include hands-on projects from the community and partner on-ground courses with online courses/schools to expose more students to these opportunities.

Those on-ground would perform the actual tasks while those participating remotely will offer consultative services. In an entirely online situation students could complete projects remotely including researching a problem and offering the best solution, with security infused into the solution design. Actual implementation may be left to the company or an on-ground class.

While ambitious, this idea can work. My courses and students are proof of its success. I have been the teacher for on-ground and online students as we completed over 115 IT and cybersecurity projects for nonprofits in Ohio, Indiana and Texas. While my on-ground students did the bulk of hands-on work, my online students offered design and troubleshooting assistance and participated from different states, countries, some while serving in the military in places like Kabul, Japan, Germany, and two were on nuclear submarines! This idea works. We even completed a project for a battered woman's shelter where the women had to perform the work and the men had to act as consultants as no men were allowed onsite.

So far, all of the work has been completed by my students while I worked for multiple educational institutions. The on-ground students usually consist of a single class for a single school but have included several online students who either lived nearby or were able to travel to the location. The remote assistance in the form of research, troubleshooting, code/plan review were often from different schools where I taught online and participated as volunteers instead of a designated course project.

This semester I had a student participate who was enrolled at a school where I do not teach as he was the significant other of a current student and he was able to provide a level of expertise the class did not possess. The team he worked with was grateful for his assistance and experience and the project progressed faster than anticipated because of it.

The application of this proposal could result in two potential applications of this concept: 1) Train teachers to facilitate their own outreach and inclusion of hands-on community projects for their online and/or on-ground classes, and; 2) Partner teachers who are online with teachers willing to participate on-ground to benefit communities, open opportunities for experience and volunteerism to their students, and offer project-based learning activities which are much more authentic and realistic than many traditional projects and research papers.

Obviously, option 1) empowers teachers to facilitate the process independently while option 2) would require a bit more coordination between faculty and partnering institutions, but I promise it is worth it!

Often, we begin the volunteer work with a risk assessment which provides the organization with the knowledge of what is needed to protect people, property, and processes. Completed projects have included planning, designing, and building networks (usually with equipment supplied by the organization, but a few times we refurbished equipment or raised money to purchase the equipment), operating system security, secure development of middleware, website development and implementation, network/application/wireless troubleshooting, funding integration (ability to accept donations), and many others.

Not every project requires a site visit. For example, this semester in my secure development course we worked on development of two websites, a mobile application, middleware for a dentist's office, and a new distribution of Linux. Some of those were real non-profit projects and others were of my creation but which could be marketed – such as the mobile application which could be sold (low cost) in the app store with all proceeds going to the cybersecurity club, and the Linux distribution would include the names of all participants as creators and be available at DistroWatch. No site visits were necessary. The class had more than 60 students including a mix of graduate and undergraduate students. The graduate students on each project served as the project managers. The project will continue through the summer.

This concept need not apply only to academic classes. On several occasions the course work was augmented by assistance from the computer club, (which I advised) which facilitated assessing donated computers, wiping hard drives, installing Linux and OpenOffice. One project with the local Rotary club had students create a resource center in Belize (yes, the projects have had international impact, too!).

I do require nondisclosure agreements and releases of liability on all sides (students and nonprofit organization). All participants receive letters on letterhead from the assisted organization thanking the student by name for their contribution (for security and privacy, the address used is that of the school). The appropriate level of jargon and specifics is included as I

write the letters and I remain the point of contact for confirmation of their efforts and experience so the nonprofit is not overwhelmed with calls for references. All students can list their participation on their resumes as volunteerism and work experience.

As proof of concept I offer the award I received in June 2017 at the Community College Cyber Summit (3CS) for Teaching Innovation in the area of Community Outreach (won under my former name: Denise Pheils) and the research behind this community project method which was presented at the 2013 ACM InfoSec Curriculum Development Conference at Kennesaw State University and was published as:

Pheils, D. (2013). Applying a Community Project Approach to IT and Security Courses. In *Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference* (InfoSecCD '13). ACM, New York, NY, USA, , Pages 79 , 9 pages. DOI=http://dx.doi.org/10.1145/2528908.2528924

Cybersecurity Law for Undergraduates

By Jeff Kosseff[1]

Abstract: Undergraduate cybersecurity programs can – and should – educate students about cybersecurity law. This Paper outlines the U.S. Naval Academy's approach to the cybersecurity law class that is required for undergraduate cyber operations majors. Although the students have no previous legal education, they grasp many of the complex laws relevant to cybersecurity professionals. A successful undergraduate cybersecurity law class provides a foundational overview of legal concepts, integrates current events, evaluates students' written and oral communication skills, and requires students to think critically about legal issues.

In 2016, the United States Naval Academy graduated its first class of cyber operations majors – 27 midshipmen out of about 1,100 graduates. Two years later, the ABET-accredited program has quadrupled in size, with 110 freshmen choosing the major.

The Naval Academy requires all cyber operations majors to complete a cybersecurity law class, usually in their final semester. I joined the Naval Academy faculty in fall 2015, and I spent much of that semester designing the new class. I spoke to cybersecurity lawyers and operational professionals in the military, civilian government, private sector, and civil liberties groups. Most of the experts agreed on a core set of topics that they would like to see in an undergraduate cybersecurity law class.

I filled a whiteboard with more than 100 possible topics, but I did not yet have a structure for the class. I faced two primary challenges. First, I needed to whittle down the list to a manageable set of topics for a semester-long course. Second, the Naval Academy is an undergraduate institution. Law school students typically can take cybersecurity law as an elective in their second or third years, after completing the required first-year classes on contracts, criminal law, torts, property, and civil procedure. Undergraduate students, in contrast, have not received that foundational legal education before enrolling in cybersecurity law.

[1] Assistant Professor, Cyber Science Department, United States Naval Academy. The views in this article are only those of the author, and do not represent the U.S. Naval Academy, Department of Navy, or Department of Defense.

I attempted to structure the class in a logical format that tells the story of what we generally conceive of as cybersecurity law, moving from broad constitutional contours to more specific laws, and concluding with international cybersecurity norms. The class is broken into five general units, each consisting of approximately three weeks of classes:

- **Constitutional Foundations of Cybersecurity Law:** Executive power; legislative power; judicial review, and constitutional liberties (First, Fourth, Fifth, Tenth, and Fourteenth Amendments).
- **Statutory Foundations of Cybersecurity Law:** Statutory authorities for government cyber operations (with a focus on Titles 6, 10, 18, 32, and 50 of the United States Code); statutory limits on government cyber operations and surveillance (Electronic Communications Privacy Act and Posse Comitatus Act); foreign intelligence surveillance (FISA, Executive Order 12333, and PATRIOT Act); and division of governmental responsibilities for U.S. cybersecurity among federal and state agencies.
- **Private Sector Cybersecurity Law:** Federal Trade Commission data security actions; sectoral data security laws; state data security and breach notification laws; data breach litigation; attorney-client privilege for cyber forensics investigations; cyber-threat information sharing; encryption and the All Writs Act; privacy law; and General Data Protection Regulation.
- **Computer Crime and Hacking Laws:** Computer Fraud and Abuse Act; state computer crime laws; Section 1201 of the Digital Millennium Copyright Act; and Economic Espionage Act.
- **International Cybersecurity Law:** Law of war in cyberspace (jus ad bellum, jus in bello, cyber sovereignty, and jurisdiction); Budapest Convention.

Because Naval Academy students have not received a first-year law school education, each section begins with a general overview of the foundational concepts that underlie the legal issues. For instance, the Constitutional Law section begins with a brief history of judicial power dating back to *Marbury v. Madison*, and the Private Sector Cybersecurity Law section includes an overview of the stages of civil litigation.

Law school classes typically evaluate student performance almost entirely based on final-exam performance. The final exam usually requires a student to identify and analyze issues in lengthy

hypothetical fact patterns. This allows the professor to evaluate a student's ability to spot legal issues, identify applicable legal rules, and analyze how those rules apply to the facts in the hypothetical. The law-school grading model does not work well for the Naval Academy, which requires grades at the six-week, 12-week, and final exam period. Nor does the model adequately evaluate other skills that we hope to teach our cyber operations majors, including presentation delivery and expository writing. Accordingly, each student is evaluated based on the following assignments:

- A hypothetical issue spotter mid-term exam
- A term paper on a current cybersecurity law issue of the student's choice, and a class presentation about the topic
- An in-class appellate argument in which students argue for and against the reversal of a district court cybersecurity-related opinion, with practicing lawyers and faculty as judges
- A final exam with 2-3 hypothetical issue spotter fact patterns
- Two in-class presentations about current events in cybersecurity law
- Class participation

I have taught nine sections of the class since Spring 2016, and have honed the material each semester to ensure it is current. Based on this experience, I conclude with the following lessons:

- Undergraduates are far more capable of learning complex cybersecurity law concepts than I had expected. This is partly because most of the students are seniors who have taken a number of challenging technical cybersecurity classes; thus, they can understand some material more easily than technological novices. For instance, when I teach the encryption dispute between Apple and the FBI, the students already are familiar with the mechanics of encryption, allowing us to focus on legal concepts such as the All Writs Act.
- Cybersecurity law is rapidly evolving, requiring constant evaluation of course topics for currency. For instance, after courts issued many Fifth Amendment opinions regarding compelled unlocking of smartphones, I added a section about the topic. Many legal issues, such as the Fourth Amendment and the Computer Fraud and Abuse Act, always will be relevant to cybersecurity law. Current event presentations help to ensure that students critically analyze new developments in cybersecurity law.

- Undergraduate cybersecurity law classes should not aim to prepare students to perform the work of lawyers; indeed, unless the graduate has a juris doctor and active bar admission, such work would be illegal. Instead, the undergraduate cybersecurity law class should expose students to the fundamental legal issues that they will encounter throughout their careers in cybersecurity, and to understand when they need legal advice. The class also should cause students to think broadly and critically about the role of the cybersecurity profession in a society of laws and norms.
- Cybersecurity education is not a binary choice between technical and non-technical subjects. The students in my class apply their technical knowledge to the relevant laws, resulting in productive discussions. For instance, when we assessed the privacy implications of the Dark Web, much of the class involved a discussion of the mechanics of TOR. Relatedly, students tell me that the cybersecurity law class causes them to think carefully about the legal implications of their technical cybersecurity research.
- The course is most effective when it forces undergraduates to critically evaluate not only how current laws shape cybersecurity, but also how future laws *should* affect the field. As future cybersecurity leaders in the private sector or government, they may have the ability to shape the rapidly evolving body of cybersecurity law.

NACE Workshop Position Statement – Cybersecurity Education and Competency Challenges

Nancy R. Mead, PhD, SEI Fellow Emeritus, CMU Adjunct Professor of Software Engineering, nrmcmu@gmail.com

Bio Sketch: Dr. Nancy R. Mead is a Fellow Emeritus of the Software Engineering Institute (SEI), and an Adjunct Professor of Software Engineering at Carnegie Mellon University. Her research areas are security requirements engineering and software assurance curricula. The Nancy Mead Award for Excellence in Software Engineering Education is named for her.

Prior to joining the SEI, Mead was a senior technical staff member at IBM Federal Systems, where she spent most of her career in the development and management of large real-time systems. She also worked in IBM's software engineering technology area and managed IBM Federal Systems' software engineering education department. She has developed and taught numerous courses on software engineering topics, both at universities and in professional education courses.

Mead has more than 150 publications and invited presentations. She is a Life Fellow of the IEEE, a Distinguished Member of the ACM, and was named the 2015 Distinguished Educator by IEEE TCSE. Dr. Mead received her PhD in mathematics from the Polytechnic Institute of New York.

Position Statement: Let us consider challenges in cybersecurity education and its associated competencies:

- Cybersecurity these days must consider much more than shoring up an existing system's defenses and applying patches.

  Although cybersecurity was once limited to such concepts as patch management, firewalls, and encryption, it has become clear that such methods are far from adequate for today's threats. Unfortunately, many managers are still stuck in a time warp that leads them to think that cybersecurity is something that only needs to be considered after a system is fielded. As a consequence, systems are developed that can never be adequately secured due to poor architecture and implementation decisions. There is a substantial need to educate people who are still laboring under these misconceptions.

  These same folks do not know what to do with graduates of modern cybersecurity programs, and relegate them to low-level positions in system administration just to fill a slot (I call this "cannon fodder"). The highly qualified individuals hired into these slots can't wait to "do their time" and find a more interesting job, and some of them even buy their way out of a contractual obligation in order to do so.

- When they hire, employers tend to look for experience in specific languages and tools, rather than more substantial competencies. Moreover, career advancement in cybersecurity seldom includes defined competencies as a consideration.

  It's probably been at least 5 years since I pointed out that classified ads do not seek individuals with substantial educational background. Instead, they advertise for expertise in specific languages, specific static analysis tools, and so on. Moreover, they don't want to train new employees, but expect them to be productive out of the box. This occurs in part because people change jobs often, and employers don't want to invest in growing the skills of people who will be gone in a year.

  On the plus side, there are some organizations who have developed competency models for cybersecurity and software assurance. How they are being used, however, is largely unknown.

- At all levels of education, there is a dearth of faculty who are qualified to teach cybersecurity.

  In attempting to transition software assurance curriculum recommendations, especially at the community college and high school levels, it is clear that there are not enough qualified faculty to do this. If the school has degree offerings in computer science or information systems, then the existing faculty can learn enough about the field to be able to teach it. However, faculty members who are

set in their ways are not necessarily motivated to change. One possible solution is to bring in adjunct faculty to teach these courses, but quite frankly, for someone in industry, adjunct salaries usually amount to what I call “charity work”. If you consider all the hours put in, the salary doesn’t even amount to minimum wage.

On the plus side, whenever software security and software assurance degrees are offered, there seem to be an ample number of students who are interested in these offerings. In undergraduate and graduate programs, more cybersecurity degree offerings exist than at the lower levels, but there is a risk that students will rush into these programs because the field is “hot”, and later as graduates, lose interest and drop out of the field, much as we saw in computer science some years ago.

- For the most part, standard sets of material for teaching a cybersecurity or software assurance curriculum at any level are not publicly available.

  Although some faculty are willing to make their material publicly available, it is often the case that the material is considered the intellectual property of the university or the individual faculty member. Individual faculty members who use the same material to do consulting or teach industry workshops are reluctant to share their materials with others who may have similar consulting arrangements. Universities may be reluctant to have material shared if they think it helps a competitor. With online and distance education offerings, any university can be considered a competitor, regardless of their physical location.

  Government-funded projects have helped to address this, but the funding is usually insufficient to support fielding an entire program, and it can’t be counted on from one year to the next. If it is done, it is usually a one-time effort, with no opportunity to refresh and modify the material at a later time. The funding, when it exists, is often used to support making course materials available “as is”, without consideration of how to make it useful to other instructors who are not teaching the exact same course at the same university. By and large, there is no data collected on how many faculty use publicly-provided material, or how effective it was, assuming measures of effectiveness even exist. Needless to say, the same applies to students who are on the receiving end. Sad to say, it’s possible to get a grant to support a single workshop, or what is otherwise a volunteer effort, but grants to support a substantial amount of work are seldom available.

- Possible solutions

  Given the challenges, it may appear that this is a nearly impossible problem to solve. However, I believe that a cooperative, appropriately funded, multi-year effort between government, industry, and academe could go a long way.

  The NICE framework attempts to address some of the issues, but it seems to be largely concerned with managing the effort, rather than developing content, and once again depends on voluntary participation and donated materials. Possibly it could serve as more than just a clearing house for materials, although it too appears to involve a revolving door of managers who are there for a year or two, and probably the funding varies from one year to the next as well. The Scholarship for Service program certainly produced a number of graduates with excellent background, although it's not clear whether it could/should continue. Ditto for the Centers of Academic Excellence. Certainly government needs to be a long-term part of the solution.

  Industry needs to recognize that this is not simply a case of telling educational institutions what skills are needed from graduates, so that they can be productive from day one. Higher education is intended to produce individuals who have learned the fundamentals that will serve them well over the course of their careers – the ability to create, learn, apply, and analyze problems, approaches, and methods that may not even exist when they graduate.

  Considering the fact that information systems and cybersecurity now concern all of us in our daily lives, educational institutions at all levels need to collaborate to support the development and delivery of appropriate course materials. This is not a time for stove-piping.

  Measures of effectiveness need to be defined and built into educational program follow-up. It is not sufficient to do something once and then declare victory. It takes resources to track graduates over a period of years, collect feedback, and use the feedback to improve present and future programs.

  All of this takes dedication, and resources. It's not something that can be tossed off in a year or two. While it is certainly the case that progress has been made, more is needed.

  [Generic reference due to word count limit! https://www.sei.cmu.edu/education-outreach/curricula/index.cfm]

Interdisciplinary Cyber Security Education

Randal Milch and Nasir Memon

New York University

NIST's National Initiative for Cybersecurity Education (NICE) is a crucial step toward remedying the Nation's undeniable shortage of "people with the knowledge, skills, and abilities to perform the tasks required for cybersecurity work." Such a workforce will include "technical and nontechnical roles that are staffed with knowledgeable and experienced people."

The NICE Cybersecurity Workforce Framework goes on to identify 7 workforce categories, which encompass 33 specialty areas and over 50 work roles. A review of the specialty areas and work roles shows that – in many crucial areas – an "integrated cybersecurity workforce" is not split between "technical and non-technical roles." Within the seemingly non-technical "Oversee and Govern" workforce category for instance, every work role in the Legal Advice and Advocacy, Strategic Planning and Policy and Executive Cyber Leadership Specialty Areas requires technical knowledge of "computer networking concepts and protocols, and network security methodologies." (K001). Similarly, every work role in the apparently technical "Securely Provision" workforce category, requires quintessentially non-technical knowledge of "laws, regulations, policies, and ethics as they relate to cybersecurity and privacy." (K003).

The question, then, is how to produce a workforce with these inter-disciplinary skills. Recent and laudable strides made to create more cybersecurity engineers at do not require a law and policy course for masters candidates on the technical track.[1] Similarly, Professor Chesney's recently published and excellent syllabus for his "Cybersecurity Foundations: Law, Policy, and Institutions" course has no technical component for law and policy students without technical training.[2]

We propose that a critical component to an interdisciplinary need is actual

interdisciplinary instruction. For two years, the authors have taught a seminar in which JD and LLM students at NYU Law School and MS and PhD students at NYU Tandon School are instructed together. The class's premise is that technology and policy are interdependent in cyberspace.

We posit that the key to intelligent application of the disparate regulatory and policy schemes with which we confront cyberinsecurity – and the basis for intelligent development of law and policy – is a thorough understanding of the technology that underlies the current and future security of the Internet. At the same time, the engineers who build products and solve problems can increase the range of policy choices if they appreciate the range of policy needs and legal/compliance requirements, including those that are inefficient or counter-intuitive from an engineering point of view.

Our seminar aims to bring the relevant technology and the current legal landscape together, for a richer understanding of each. The seminar seeks to impart the following key cybersecurity engineering concepts:

- Understand threat, vulnerability and risk;
- Basic concepts of security - confidentiality, integrity and availability, and the means for achieving these properties in a system;
- Basic concepts related to how the Internet works - packet switching, routing, DNS, etc.;
- Understand how anonymity can be provided while communicating on the Internet and why attribution of attacks is difficult;
- Problems related to identity and authentication.

And the following key cybersecurity law and policy concepts are taught:

- How rules are made with respect to cybersecurity and who makes the rules – legislators, regulators and private groups;
- The roles and responsibilities of the government and private parties in

protecting networks;

- What companies are obligated to do with respect to cybersecurity;
- Issues surrounding voluntary information-sharing (public/private and private/private);
- How regulation and private civil litigation are defining "reasonable" cybersecurity measures;
- Obligations to provide information to and cooperate with government (intelligence, law enforcement, data vs. metadata):
- Data privacy regulation (EU vs. US) and its impact on cybersecurity (e.g. insider threat monitoring).

Students are placed in interdisciplinary groups to tackle problems from both technical and legal/policy angles. Responses to the course have been favorable, and it is clear that both the engineering and the law students take away a new and valuable literacy with one another's chosen fields. It is also apparent that the difficulties in cross-training are not equal. It is easier to provide engineering students with instruction in law and policy than it is to provide law students will little or no technical background with meaningful technical instruction.[3]

Efforts at the graduate level, however, ignore the large cybersecurity workforce already in place. Steps must be taken to provide existing cybersecurity professionals without interdisciplinary training with a route to obtain the knowledge they need to excel in their role. Based on the success of the graduate-level seminar, NYU is seeking to meet this need through a new Executive MS in Cybersecurity Risk and Strategy offered jointly by NYU School of Law and NYU Tandon School of Engineering.[4] The one-year program is intended for experienced professionals from a range of backgrounds who seek to deepen their understanding of cybersecurity risk and strategy. This program will create managers with the integrated expertise needed to play a leadership role in the field.

The MS in Cybersecurity Risk and Strategy program is a 30-credit executive MS management degree incorporating both online courses and blended-learning modules. Over a 12-month period, participants attend three residential sessions consisting of five days per session. Between residential periods, students are expected to study 10-15 hours per week in online and blended-learning formats. Semesters are divided into three phases: online introduction, in-class residency, and online implementation.

In order to ensure a common foundation for students from widely disparate backgrounds, MS-CRS students must, before starting their credit-bearing courses, pass on-line "bridge" courses in U.S. Law and in the technical Foundations of Cybersecurity. Each semester includes a 3 credit, core engineering course (Information Security and Privacy, Network Security, and Information Systems Security Engineering and Management) and two law or policy courses (such as Information Privacy Law, Cybersecurity Governance and Regulation, Cyber Crime and Innovation Policy) bearing a total of 5 credits. Spanning all three semesters is a 6 credit, team-based "Integrative Cybersecurity Management" Capstone Project.

Author Bios

Randal Milch is the Co-Chair of the NYU Center for Cybersecurity, a Distinguished Fellow at the Center on Law and Security, and a Professor of Practice at NYU School of Law

Nasir Memon Nasir Memon is a professor in the Department of Computer Science and Engineering at NYU Tandon. His research interests include digital forensics, biometrics, data compression, network security and security and human behavior.

[1] On-line students in the Georgia Tech program who chose a "Policy specialization" would be hard-pressed to avoid at least one law or policy course.

[2] Importantly, Professor Chesney hopes to attract "grad students . . . in business, engineering, and computer science" to his course.

[3] Law students *with* a technical background, however, are perhaps the most adept at mastering the combined material.

[4] The authors serve as Faculty Co-Directors of this new Program.

THE REVIVAL OF THE APPRENTICESHIP: A NEW APPROACH TO CYBERSECURITY EDUCATION (NACE) WORKSHOP CONCEPT PAPER

by

Lauren Neely, JD

The job titles in cyber security vary, as do the skills, experience, and tools needed to successfully perform the duties demanded by those titles. The skill set that might prepare a potential employee to be a Security Analyst will not be the same skill set needed to work as a Security Software Developer or Engineer or a Security Consultant. For instance, a security software developer may require a greater knowledge of programming languages, web development, agile methodologies, and cloud computing. For this reason, I propose that the best way to address the levels of education and training needed for future cyber security professionals and the cyber security labor supply issue is through the revitalization of the apprenticeship model of workforce development. Programs such as the National Science Foundation's Scholarship for Service program have made important contributions for students who will work for federal agencies upon completing their education, but a similar effort needs to be embraced by industry. Apprenticeship programs are unique in that they often align education with on-the-job training and have the added benefit of ameliorating a persistent problem facing entry-level or career transistioners looking to move into the industry. In order to get a job they need experience, but they cannot get experience because employers can ill afford to take a chance on untried entry-level employees. Sources have recognized the current disconnect between the claims of thousands of unfilled cyber security positions and the new graduates and potential employees who have tried to break into the field unsuccessfully because they lack the requisite experience.[1] Apprenticeship programs can fill this gap.

According to the U.S. Department of Commerce,

"Apprentice programs work – not only because they help employers find exactly the trained talent they need but because they help people quickly enter a field, without college debt or an exhausting job search. Apprentices tend to be loyal workers because their employers have invested in them both on the job and through educational assistance to help advance their careers. This has shown to reduce employee turnover rates and increase morale."[2]

The National Initiative for Cybersecurity Education (NICE) led by National Institute of Standards and Technology (NIST) and at US Department of Labor's Office of

[1]Tripwire, The State of Security: News, Trends, Insights. "Talent Shortage Sanity Check." https://www.tripwire.com/state-of-security/risk-based-security-for-executives/connecting-security-to-the-business/talent-shortage-sanity-check/ retrieved April 30, 2018.
[2]U.S. Department of Commerce, Apprenticeship Works for the IT Industry, https://www.commerce.gov/news/blog/2018/01/cybersecurity-apprenticeships-enhance-cybersecurity-infrastructure retrieved April 30, 2018.

Apprenticeship offers support and guidance for those looking to build an apprenticeship program, but to date only a handful of these programs are in operation. It is incumbent upon local employers, educational institutions, and cyber security professional organizations to work together to create viable apprenticeship programs. These programs will serve to alleviate the labor shortage and allow for a more diverse cyber security workforce by actively recruiting women and minorities as apprentices.

Lauren Neely received her J.D. from the University of Houston Law Center. Upon graduating from law school, Lauren worked for a commercial real estate advisory firm for several years before deciding to return to the public sector and her alma mater, the University of Houston. Lauren served in several capacities during her return stint to the University of Houston and is the former Assistant Director of the Hobby School of Public Affairs. In 2017, Lauren joined the University of Houston Law School Street Law Program as a co-instructor. Lauren is a member of the State Bar of Texas and is currently pursuing a Master's in Cyber Security Operations and Leadership at the University of San Diego.

Futuristic Cybersecurity Education and Workforce Development Initiatives

A Proposal by Amos Olagunju, IT Professor

St Cloud State University, St Cloud, MN

0. Foreword

The survival of the current and future cybersecurity workforce will depend on effective strategies for the recruitment, retention, and continuous educational training of diverse students in high schools, two and four-year academic institutions. This proposal provides justifications and advocates initiatives for continuous successful recruitment, retention and training of diverse students for sustaining cybersecurity workforce.

1. Recruitment

Four-year academic institutions should form partnerships with local or nearby high schools and technical and community colleges, to sustain the recruitment of diverse students for associate or bachelor's degrees in areas relevant to cybersecurity. Today many academic institutions promote and support experiential training for students in the areas of computer science, information technology, and cybersecurity. Essentially, current computer science, cybersecurity and information technology degree programs that mandate experiential learning or capstone requirements should engage and mobilize more students to serve as role models for recruiting students from high schools and two-year institutions. College students should be guided by faculty and staff members to design academic and co-curricular skill-enrichment mathematics and computing activities for motivating youngsters to pursue bachelor's degree programs in cybersecurity and related areas. The enrichment activities should be delivered by college students to high schools on convenient periodical schedules.

Faculty members at four-year academic institutions ought to sign more articulation student transfer agreements with two-year institutions that offer associate degrees in areas related to cybersecurity education. Moreover, faculty members at two and four years institutions in areas of cybersecurity should meet periodically, to review and recommend changes in the educational training of students at two-year institutions for successful careers.

2. **Retention**

Clearly, it is not enough to recruit diverse students into cybersecurity programs without a strategic plan to cope with students who end up struggling with core courses in areas such as mathematics and computer programming. A comprehensive cybersecurity program in associate or bachelor's degree ought to have alternative plans for guiding students with deficiencies in mathematics, scripting, programming, and/or installation and applications of cybersecurity tools to success. Retention strategies might include the use of currently high-achieving cybersecurity majors or alumni or industrial partners to mentor and serve as role models to future cybersecurity experts. Retention of minority students in cybersecurity programs might be considered intrusive, but there is reason to believe that a carefully outlined alternative plans for guiding students with various academic, family, social and financial issues, will promote more diverse students for the cybersecurity workforce.

3. Cybersecurity Skill Training Requirements

The question naturally arises on the skills required for graduates with two-year or four-year degrees in cybersecurity. Should associate and bachelor's degree programs in cybersecurity be designed and offered based on the existing and future anticipated faculty strength? Regardless of the faculty strength what skills should graduates with associate or bachelor's degrees in cybersecurity demonstrate upon graduation, and perhaps in long-life learning?

In agreement with the ABET requirements for the accreditation of current and future cybersecurity programs, herein are long-life skills for future cybersecurity training:

Student learning outcomes for cybersecurity majors should mirror the ability to:

1. Write correct, well-documented and readable programs.
2. Describe and use networks.
3. Describe and use operating systems.
4. Articulate ethical, professional, and legal standards of behavior.
5. Communicate effectively in written and oral exchanges.
6. Design and implement secure network architecture based on security policies.
7. Identify and correct security weaknesses in operating systems, networks, and applications.
8. Demonstrate understanding of theoretical foundations of security by solving problems.

9. Design and implement effective defensive and offensive strategies in cyber security.

But, what kinds of courses should be designed to satisfy the current and future needs of cybersecurity workforce? Here are a few examples:

- A Course in Firewall and Penetration Testing might include Knowledge of common network tools:
    - Knowledge of Computer Network Defense and vulnerability assessment tools, including open source tools, and their capabilities
    - Knowledge of Defense-In-Depth principles and network security architecture
    - Knowledge of general attack stages Knowledge of network security architecture concepts including topology, protocols, components, and principles
    - Knowledge of penetration testing principles, tools, and techniques
    - Skill in applying host/network access controls
- A Course in Offensive and Defensive Security might cover:
    - Knowledge of different classes of attacks
    - Knowledge of front-end collection systems, including network traffic collection, filtering, and selection
    - Knowledge of host/network access controls
    - Knowledge of incident response and handling methodologies
    - Knowledge of intrusion detection system tools and applications
    - Knowledge of network traffic analysis methods
    - Knowledge of the common attack vectors on the network layer
- Applied Cryptography
    - Knowledge of cryptology
    - Knowledge of encryption methodologies
    - Knowledge of network access, identity and access management
- Database
    - Knowledge of database management systems, query languages, table relationships, and views
    - Knowledge of database theory
    - Knowledge of query languages such as SQL

    - Skill in developing data models
    - Skill in generating queries and reports
    - Skill in maintaining databases
    - Skill in optimizing database performance
- Operational Safeguards
- Knowledge of policy-based and risk adaptive access controls
- Knowledge of current and emerging threats/threat vectors
- Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins
- Knowledge of system and application security threats and vulnerabilities
- OSI Layer Security
- Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol (TCP) and Internet Protocol (IP), Open System Interconnection Model (OSI), Information Technology Infrastructure Library, v3 (ITIL))
- Knowledge of IA principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation)
- Knowledge of network security architecture concepts including topology, protocols, components, and principles
- Knowledge of VPN security
- Skill in securing network communications
- Computer Forensics
- Knowledge of anti-forensics tactics, techniques, and procedures
- Knowledge of basic concepts and practices of processing digital forensic data
- Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data
- Knowledge of seizing and preserving digital evidence
- **Security Policy and IT Risk Management**
- Knowledge of Computer Network Defense policies, procedures, and regulations
- Computer Networks
    - Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services

Summary

The industry is already infusing DevOps tools and agility into business operations. The need exists to develop case-based projects for training the future cybersecurity workforce about agile skills and rapid applications and network monitoring using DevOps tools. If I have the opportunity to participate in this panel discussion of the long-overdue recruitment and retention of the Cybersecurity Workforce, I will be willing to demonstrate creative projects that can be used to motivate, recruit, and retain more students into the current and future cybersecurity workforce.

Bio Sketch of Amos Olagunju

Amos Olagunju is a professor in the Computer Science and Information Technology Department at St. Cloud State University (SCSU) in Minnesota. He previously served as the interim dean of undergraduate studies at SCSU. Under his leadership, SCSU experienced the highest levels of enrollment, retention and graduation of students for minority students in STEM areas. He has served as the School of Graduate Studies Dean and Chief Research Officer at Winston Salem State University. A faculty fellow and later a senior faculty fellow selected jointly by the American Society of Engineering Education and the Navy, Amos developed manpower mobilization and data-mining algorithms for monitoring the retention behaviors of personnel. Under the leadership of Amos as a Professor and Chair of the Computer Science Department, Delaware State University established a reputable computer science degree program for minority students. As a visiting scholar at Michigan State University, he investigated the barriers to the retention and graduation of minority students in computer science and published a solution manifesto for international audience in computer science education. Amos is an ABET Program Evaluator. He has participated in the Carnegie African Diaspora Fellowship Program and the Specialist Fulbright Scholar Program.

Dr. Stephen R. Orr IV is currently the National Security Agency (NSA) visiting Professor for Cyber Security Studies at the United States Naval Academy. He holds a Ph.D., M.S., and B.S. degree in Computational and Information Sciences. Dr. Orr has held analytical, technical, operational, and leadership positions at both Headquarters and the field. His expertise and career has focused on offensive and defensive cyberspace operations. Most recently, Dr. Orr was part of a team that won NSA's prestigious Deckert/Foster Award for Excellence in SIGINT engineering.

Dr. Orr's most recent assignment was the Executive Director of J3, Operations for United States Cyber Command. In this capacity he was responsible for directing command operations spanning from future planning, through operations execution within the authorized computer network operations mission space.

Dr. Orr's research interests include the intersection of cybersecurity and human factors, cyber effects, and the application of emerging technologies.

This proposal attempts to address the challenge of what a follow on Scholarship for Service (SFS) could look like in the twenty years since it was first established, while addressing multiple general topic areas to cybersecurity education. It is through this proposed academic construct that private and public sector challenges could be addressed. Simply put, it is proposed that we evolve the **centers of academic excellence construct to focus on the "*at least three dozen specializations*" that exist in the cybersecurity discipline**. Diversifying the expertise at any one academic center of excellence has the ability to produce many students that are average at everything, and good at nothing. By restructuring the fundamental institutional model, these centers of academic excellence **and specialization** would create a monopoly on **producing expertise** in one of the many subdisciplines of cybersecurity. In turn, students would graduate with the broad liberal arts education that inspires creativity and critical thinking, complemented with specialized skills to meet the private and public sector cybersecurity challenges. Furthermore, this institutional construct provides a gateway for solving the more general topic areas of cybersecurity education.

The National Security Agency (NSA) originally created the Center for Academic Excellence in Information Assurance Education (CAE-IAE) in 1998, with the Department of Homeland Security (DHS) joining as a partner in 2004. Since that time te CAE in IA Research component was added in 2008 to encourage universities and students to pursue higher-level doctoral research in cybersecurity. Later, the CAE-Cyber Operations program was established, which focuses on technologies and techniques related to collection, exploitation, and response. This construct has, and continues to pay dividends to enhance the national security posture of our Nation. **The specialization designator allows academia to take the lead by voluntarily constructing a monopoly on specialized cybersecurity education**. This evolution would further enhance the NSA and DHS sponsored Centers of Academic Excellence, while also "future-proofing" the education we provide.

To be clear, it is not proposed that these institutions would **only teach** any one of the subdisciplines of cybersecurity. Nor that there would be only once academic institution to focus on any one specialization. **Specialization requires a solid foundation and core competencies**. For example, a fundamental understanding of computational and information concepts such as programming, operating systems, and networking; policy, legal, and ethics would be necessary. Each of the documented specializations would further focus on these

particular areas allowing the academic center of excellence to be designated as producing graduates with a particular specialty. However, given this is a dynamic field it is guaranteed that the specialization requirements of tomorrow will not be the same as the specialization requirements of today. This proposal allows for academic institutions to adapt to meet the specialized requirements without significantly disrupting their entire academic program, as the fundamental core competencies will remain the same. Collectively, academia would meet the demands of private and public institutions today, while having the ability to adapt and change to the dynamic needs of the future. **Thus, "future-proofing" the academic education through specialization is achieved by adapting to the cybersecurity challenges of today and tomorrow, while providing a core foundation in computation and information science concepts**.

The proposed academic centers of excellence and specialization **creates a natural opportunity to partner with cybersecurity vendor-neutral training and certification providers, or supplanting them by meeting the needs of the market they currently fill**. Vendor-neutral certifications typically validate a candidate's unbiased knowledge or skills of a particular technology principles. This is done through traditional tests and hands-on, skill-based scenarios. The specialization designator lends itself to providing more specific, short-term knowledge and skills to meet the demands of today. This specialization, combined with a traditional broad understanding of computational and information sciences provides a win-win-win scenario for the student, academia, and industry. An academic institution that currently offers a version of this proposal is the University of Maryland University College (UMUC). They offer technical programs that combine broad understanding of fundamental computation sciences with cybersecurity training and certification to meet industry demands. Creating academic centers of excellence and **specialization** could build and improve upon this model while increasing value of a college education. **Specialization through academic centers of excellence creates centers of gravity to address the mix of education methods, industry practice, and government needs**.

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.

Onramp to cybersecurity Labor Pipeline through K12 Classroom Education

Meg J Ray
Teacher in Residence
Cornell Tech

Tim Winston
Principal, PA-QSA(P2PE), CTGA, CISSP, CISA
Coalfire Systems

Key to solving labor supply issues in cybersecurity is a strategy that begins well before college. To achieve a diverse pipeline of cybersecurity professionals and a populace educated in basic data privacy and security concepts, we must build and fund a coherent K12 strategy that makes sense in our current school system and brings together the expertise of cybersecurity and education specialists.

The primary need is a future-proof and readily available labor pipeline in the US. The impact of Moore's Law on all current technology spaces (ie. mobile devices, cloud computing, IOT) not only applies to increasing computational power but more generally to the exponential expansion of all types of capabilities. Given this circumstance, future proofing our workforce will not be about anticipating technological development, but about preparing professionals who can assimilate new technologies quickly, apply foundational concepts in novel situations, and are fluent in metacognitive skills. Although students will still require areas of technical proficiency, this mindset requires a shift in our approach to education. Students will still need to develop one or two areas of technical proficiency. This will allow incoming professionals to fully appreciate how to secure and apply cybersecurity principles, to one area that they understand deeply before generalizing to a wide range of technologies.

Technical roles are not the only need to be addressed in cybersecurity labor supply. The technically oriented attacker and defender roles may be the first and only ones that come to mind, but there are many others on a team that are vital to supporting these roles. In the cybersecurity field we also need skilled project managers, educators, designers, and grant managers. People who do not have the interest or opportunity to pursue the engineering side, need to know that there are still critical careers in cyber security where they can make a crucial contribution.

A secondary need that K12 education can address is a cybersecurity literate population. This type of general literacy can only help the efforts of cybersecurity specialists on a broad scale. A better understanding of security and privacy is more important than ever: policy makers at all levels, developers and data scientists, CEOs and CFOs in all industries, and voters. It is of vital importance that individuals across industries understand the value of, and threat to, their personal and professional data. In this way individuals would better understand and support the need to properly protect information.

We can lift important lessons from recent efforts to broaden access and awareness in STEM and CS education. Early positive math and science experiences and career awareness, especially at the middle school level, is important to recruiting interest particularly for underrepresented student populations (Maltese & Tai, 2011; Moakler & Kim, 2014). Leaving relevant classes and experiences only to those who opt in, excludes large numbers of talented students. Barriers include issues of student identity and obstacles to access, such as needing to hold an after school job or attending a school that does not offer AP classes (Margolis, 2008; Wang & Degol, 2013). To address these needs, we propose a multi-pronged approach touching all levels of K12 education.

First, all children need a basic understanding of how the digital world works. As outlined in the K12 CS Framework, they should understand the basics of computers, networks, and data. In order to recruit interest in cybersecurity and prepare students for required classes, it is important that they do not leave high school with the vague idea that it works "somehow" or by "magic." Children's innate temptation to misuse things can actually be a positive indicator for both STEM and specifically security. Rather than simply correct the impulse - it can identify the aptitude and redirected to the importance of building and testing securely. These concepts can be fit into CS, technology, or science classes. Elementary school students are introduced to these concepts through the use of stories and physical activities that model computing processes. As students move up, they are able to learn lower level concepts and incorporate them into projects that reflect real world contexts.

In middle school, many schools begin to teach digital citizenship. There is a tendency in CS education to draw a hard line between technology/digital citizenship and computer

science/coding. We need to soften this line and reboot our middle school curriculum. Digital citizenship education 2.0 must involve more than anti-cyberbullying campaigns. Students should learn web safety as well as web development. They learn to not give their personal data to strangers, but should also learn how their data is tracked with routine web use and how to secure and protect their own data.

In high school, it is appropriate for all students to learn and think about the current and historical context of cybersecurity. In social studies classes, units should be supplemented to include themes related to surveillance, privacy, protecting our capabilities, ethics, etc. They should understand personal and national security as themes in wartime and peacetime and how historical events have impacted current issues.

In high school, we can broaden current CS learning for students who are taking higher level math and CS courses to prepare for STEM careers. CS classes need to incorporate opportunities for students to have counter functional experiences, by “breaking” each other's work and by finding new use cases. This “make it, then break it” approach also addresses practices and metacognitive skills in the K12 CS Framework that are more difficult to teach. For example, we want students to understand that projects are never just done. There are always iterations that can be made based on need and context. We also want students to know that making something work technically is just as important as developing soft skills like problem solving, self-reflection, and project management. We can open the doors of CS experiences such as robotics clubs and engineering classes to a wider group of students by explicitly creating and valuing roles project manager or publicist.

In order to make this K12 strategy a reality, two areas need to be addressed. First, we need quality curriculum disseminated effectively to teachers. This type of curriculum is best developed within partnerships between education and cybersecurity experts. Disseminating curriculum means building partnerships with trusted education websites across disciplines. Teachers cannot teach curriculum that they do not know about. Second, we need to train teachers. Unfortunately, cybersecurity is an area about which many lay people hold misconceptions. Looking again to recent developments in CS education, we know that professional development is a complex problem to address due to issues of scale, fidelity, and

teacher interest and capacity (Pollock, et al., 2017). However, a blend of online and in-person training as well as partnerships with school districts, non-profits, industry, and universities, makes it possible. The approach we have outlined is built for minimal change in the school day and is a relatively light lift, based on doable changes such as supplementing lessons or units in existing curriculum. If stakeholders in K12 education, universities, and industry work together, it is possible to create an effective primary and secondary education strategy that will be the cornerstone of cybersecurity literacy in the general population and play a key role in increasing and diversifying the cybersecurity labor pipeline in our country.

BIO SKETCH

Tim Winston | PA-QSA(P2PE), CTGA, CISSP, CISA | Principal
Tim Winston is a Principal Consultant in Point-to-Point Encryption (P2PE) and encryption key management at Coalfire Systems. Tim is an information security and risk professional with over 35 years of experience in all aspects of information technology. He has extensive experience in software development, networking, access control systems, identity management, cloud platforms, and has provided cyber security expertise to the largest cloud platform providers, payment terminal manufacturers, encryption service providers, payment service providers, government agencies, biomedical research organizations, healthcare solution providers, critical infrastructure providers, e-commerce service providers, and retailers.

Meg J Ray
Meg Ray is the Teacher in Residence at Cornell Tech. Meg is responsible for the implementation and design of the Teacher in Residence program, a coaching program for K-8 CS teachers in New York City schools. Meg served as a writer for the Computer Science Teachers Association K-12 CS Standards and as a special advisor to the K12 CS Framework. She is an experienced high school computer science teacher and special educator, and also taught graduate-level education courses at Hunter College. Previously, Meg directed the design of a middle school CS curricula. She researches CS teacher training as well as access to CS instruction for students with disabilities. Her work is published in academic journals and conference proceedings. She has a forthcoming intro to programming book aimed at middle and high school students. Meg holds a Master's of Science in Special Education from Hunter College and a Graduate Certificate in Blended Learning and Computer Science Instruction from Pace University.

CITATIONS

K–12 Computer Science Framework (2016). Retrieved from http://www.k12cs.org.

Maltese, A. V., & Tai, R. H. (2011). Pipeline persistence: Examining the association of educational experiences with earned degrees in STEM among U.S. students. Science Education,95(5), 877-907. doi:10.1002/sce.20441

Margolis, Jane. (2008). Stuck in the shallow end : education, race, and computing. Cambridge, Mass. :MIT Press.

Moakler, M. W., & Kim, M. M. (2014). College Major Choice in STEM: Revisiting Confidence and Demographic Factors. The Career Development Quarterly,62(2), 128-142. doi:10.1002/j.2161-0045.2014.00075.x

Pollock, L., Mouza, C., Czik, A., Little, A., Coffey, D., & Buttram, J. (2017). From Professional Development to the Classroom. Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education - SIGCSE 17. doi:10.1145/3017680.3017739

Wang, M., & Degol, J. (2013). Motivational pathways to STEM career choices: Using expectancy–value perspective to understand individual and gender differences in STEM fields. Developmental Review,33(4), 304-340. doi:10.1016/j.dr.2013.08.001

New Approaches to Cybersecurity Education (NACE) Workshop

What are some good ways to "future-proof" the education we provide?

Bridge Jobs (NICE Work Roles) and Course Offerings

There is an opportunity to measure the gap in program offerings and existing job functions by mapping the *NICE Cybersecurity Workforce Framework's* (NICE CWF) Work Roles to NSA/DHS National Centers of Academic Excellence in Cyber Defense (CAE CD) Focus Areas (FAs) or the more granular CAE Knowledge Units (KUs). This mapping will allow SFS to measure if there is sufficient coverage of the tasks, knowledge, skills and abilities for a given degree plan to allow a graduate to fill and succeed in a NICE Work Role.

Creating this mapping will highlight any gaps between CAE CD curricula and existing jobs. As Work Roles and Focus Areas are aligned, programs can offer students predefined *Plans of Study* (curricular paths) that are tied to a job function in the cybersecurity workforce. Maintaining this mapping will also provide an opportunity for programs to ensure that course offerings remain up-to-date with job offerings. As new NICE Work Roles and CAE Focus Areas are created and refined, this mapping will allow programs across institutions to adjust their course offerings accordingly and offer new *Plans of Study* where their courses offer the appropriate coverage. While this does not completely capture all jobs and roles in industry, it provides a starting point for institutions to measure "coverage".

Encourage External Learning Opportunities

Xavier Univeristy's Williams College of Business created a *Business Profession Passport Program* that "provides a structured way in which undergraduate students can gain knowledge, skills and networking contacts to complement their education and to educate them on the fundamentals of the working world [4]." This same concept and mechanism can be adopted for cybersecurity students. To account for the pace of change in cybersecurity, programs should consider creating a passport-like program that encourages students to go outside of their coursework and programs to seek out other opportunities, challenges and learning opportunities.

Programs can define specific activities or provide general categories, but the goal is to get students to seek out resources and opportunities that the program might not offer or does not have the capacity to offer in the near term (prior to the student's graduation). This passport concept also reinforces the importance of seeking out new opportunities and being in a mode of constant learning. Cybersecurity changes rapidly and, sometimes, at a pace faster than an employee's organization or student's program can adapt and marshal adequate training and resources to help the employee or student succeed. These activities might include:

- serve as an officer in a cybersecurity student organization or external organization
- obtain a certification (C|EH, OCSP, Security+, etc.)
- attend a conference, talk, colloquium or presentation
- create a presentation for a local businesses group around cybersecurity
- work with a local business to better secure their systems and assets or provide training
- co-author a paper with a faculty member
- create and maintain a security blog

- learn a new programming language
- complete an internship or co-op
- create and host a capture-the-flag (CTF) event
- create one or more demonstrations and presentations to teach fellow students and faculty a new skill or technology
- create a module or series of modules that can be incorporated into a new or existing course

Programs can modify the passport idea and attach "points" to activities based on difficulty or work-effort required to complete the task. Students could be required to earn a minimum number of points on their passport prior to graduation. Again, the goal is to supplement the coursework with other learning opportunities. Learning outcomes and objectives can be created in advance to tie the external learning opportunity with measurable outcomes.

Responding to Changing Workforce Demands

One of the benefits to using a *Plan of Study* for each student is the flexibility they offer. If courses are under development or are out-of-date, programs can adjust Plans of Study to provide students appropriate coursework that meets their educational goals. Additionally, programs can use the passport program, referenced above, to fill in gaps as curriculum is updated and developed.

Along with program flexibility, cybersecurity programs should look at the "Executive in Residence" model to help bridge gaps between industry and the classroom. For programs focused on producing graduates with more technical skills, development of a "Technologist/Specialist in Residence" might be more appropriate. Regardless of the terminology used, the goal is to bring in individuals working in organizations with experience using tools and techniques currently in practice. Programs can leverage these

individuals by having them teach and develop courses, mentor students, partner with industry, collaborate with faculty and provide input on curriculum.

Looking to bring in a technologist or executive would also allow the program capacity for development activities that both faculty and students could benefit from. Higher education focuses heavily on teaching and research and development should be added to the mix. The rapid pace at which technology changes may outpace what we research and teach and having a technologist may help a program grow new skill sets and expose students to new technologies not currently integrated into the curriculum.

Curriculum Development and Access to Resources

Should SFS institutions partner together to secure agreements with security and IT vendors to acquire software and hardware for use in course work and course infrastructure for a heavy discount or for free? Essentially create a *SFS School Consortium* whose members prioritize needed resources and work to secure those tools for students and faculty.

Lastly, SFS institutions should consider developing and using open-source courseware that maps to CAE KUs and CAE FAs. For institutions that have expertise in an area and have a quality offering, SFS students should have access to that content, regardless of where it is housed. Measuring quality and creating a platform to share courses would take time to spin up, but this would allow SFS students to leverage the best courses across the SFS ecosystem benefiting the SFS students' employers, too.

About the Author

Eugene Rooney is an Analyst/Programmer III and Adjunct Faculty member at the University of New Mexico's Anderson School of Management. Eugene earned a B.S. in Computer Engineering with a Minor in Economics and a MBA from the University of

New Mexico. Prior to his current role at UNM, Eugene worked at Century Link (formerly Qwest Communications), Sandia National Laboratories and UNM's Center for Development and Disability.

In his current role, Eugene provides reporting and forecasting for school leadership along with web application development and system administration duties. He was also actively involved in securing UNM's CAE-CD and CAE-R (re)designations the last 2 cycles. In his role as an adjunct faculty member, Eugene is looking forward to teaching *Windows Scripting and Automation (PowerShell)* and *Cybersecurity Competitions* in the Fall 2018 semester to undergraduate B.B.A. Management Information Systems (MIS) students and M.S. in Information Systems and Assurance (MS ISA) students.

References

[1] Baron, Ethan. "Executives-In-Residence: Filling A Business School Education Gap." Poets & Quants, Inc. May 2005. 12 April 2018 poetsandquants.com/2015/12/04/executives-residence-filling-business-school-education-gap/.

[2] Bennis, Warren, and James O'Toole. "How Business Schools Lost Their Way." *Harvard Business Review, Harvard Business Publishing*. May 2005. 12 April 2018 hbr.org/2005/05/how-business-schools-lost-their-way.

[3] "The Business Profession Passport." *Xavier University Williams College of Business*. 2017. 12 April 2018 www.xavier.edu/williams/business-profession/documents/Passport2017.pdf.

[4] "Business Profession Program." *Xavier University Williams College of Business*. 2018. 12 April 2018 www.xavier.edu/williams/business-profession/.

The Post-Millennials Have Arrived!

New Approaches to Cybersecurity Education

Julie A. Rursch

The Pew Research Center last month signaled that the post-Millennial cohort (born 1997-present) is the latest generation [1] we will need to adapt course content for in higher education. As compared the Millennial generation which experienced the Internet boom, the post-Millennials are "always on" and "always connected." Their world has always had access to social media and on-demand entertainment. Conversations can be held at any time, at any place, with anyone. These are the students we want to attract to fill cybersecurity careers.

One of the problems we have generally in education is, since many are likely part of the Boomer (born 1946-64) or Gen X (born 1965-80) generations, is that we teach linearly, processing one thing completely before moving on to the next while the Millennials (born 1981-96) and now the post-Millennials multi-task their thoughts and actions. As educators we have started to employ active learning activities in the classroom; think-pair-share (small group discussion), peer instruction exercises where one student is the "expert" and shares his/her knowledge with others. And, these activities work well in cybersecurity.

However, where we still are struggling is with providing students the ability to see how they can apply the skills being learned in the classroom, in the laboratory, and through homeworks in the after-college world. We know the post-Millennial generation is outcome-oriented. They need to be able to see the skills built through their classroom topics connect to future use of skills. Those of us who stand before them, construct the labs, and write the homework assignments tend to break the assignments and lectures into digestible pieces and forget to tie them all together with a final project or an overarching goal as we just work linearly through the week-by-week topics. We need to give students the bigger picture and help them see how the little part they are working on each week fits into their after-college goals.

As an example, let's look at developing a realistic, hands-on experience with SQL injections, the number 1 item on the OWASP Top 10 List, to provide personal experience and connections to the real world. As faculty we can easily demonstrate the SQL injection concepts in class, both in code and as an active demonstration. We can ask them on an exam how to prevent SQL

injections which should result in some answer like sanitizing, validating, and escaping the data. This works at Bloom's lowest level, knowledge. However, if we give them each a web server, tell them they are the administrator for that web site, and have them do both pentesting on their own server (so checking for all of the Top 10, network, and OS vulnerabilities), as well as a code review, they can more clearly see how the classroom experience ties to the after-college world. It also moves them into the application and sometimes analysis level of the taxonomy. I have had students tell me that they have had SQL injections demonstrated in a previous database class, but they never understood how to prevent it until they had the opportunity to try it on their own with their own web servers. And, if giving students the entire web site is too much all at once for the class level, we can start with code snippets that are contrived for the students' ease of learning and then use similar code in the overall web site to help them make the jump to the larger picture.

Similarly, giving students an entire network that is filled with vulnerabilities and letting them have the opportunity to evaluate, remediate, and then reevaluate gives them a realistic multiple machine environment in which to work. Again, there may have to be smaller pieces of the experience given to them at first and then give them the full network as a final project with similar problems. The point of both of these examples is to give them an experience that is as realistic as possible.

Further, every time a new topic is introduced in the classroom or lab a "current event" can be included. We seem to have no limit on real world cases to build our arguments. The perfect example this past semester was using Atlanta and their ransomware problems which not only allowed discussion of ransomware, but also discussion of good disaster recovery practices and the need for business continuity plans. The latter two are good business management practices that we don't always cover in cybersecurity courses. "Current events" can easily frame the week's topic in the classroom, lab, or homework.

Now, the realistic scenarios are difficult for faculty to generate and take a lot of time and energy. Likewise, faculty do not get rewarded for good teaching. They get rewarded for papers and conference attendance, even lecturers. So, there needs to be a shift in higher education to

value the realism added to the classroom and to recognize the demands post-Millennial students are making for this kind of classroom experience.

The second issue that we need to address is the adversarial feeling in cybersecurity curriculum. To date, many of the extracurricular activities, and to a lesser extent the hands-on activities in the labs or homeworks, tend to focus on an attack mentality. As an underrepresented population, whether gender or ethnicity or other, it can be hard to put yourself into that role. We are already in the minority and then to work with cybersecurity there is a certain level of bravado that occurs with competitions and events like capture the flag or build and defend events. Even seemingly innocuous things like rank ordering teams or people in event can reduce someone's self-efficacy and, therefore, their interest in cybersecurity. Additionally, when I have been in meetings where these kinds of objections are raised I was basically told the students (in the case I am thinking about, girls) needed to, "Toughen up, buttercup!" That is not an acceptable answer. We come at cybersecurity from many backgrounds and many experiences. We won't attract a diverse population if we are chastised for offering a different view.

Finally, there isn't enough reflection in current cybersecurity education. Even if we are doing a good job and providing post-Millennial students with outcome-oriented projects where they can build future use skills, we don't have them spend enough time thinking about how what they just completed related to their major, relates to career choices, and relates to what they need to improve upon. Simple reflection questions added into the weekly assignments that ask students to put what they just completed into the larger world context is also valuable in helping them understand the tasks role in the real world.

[1] M. Dimock. (2018, March 2). *Defining generations: Where Millennials end and post-Millennials begin*. Available: http://www.pewresearch.org/fact-tank/2018/03/01/defining-generations-where-millennials-end-and-post-millennials-begin/

Suggestions for Addressing the Changing Needs of the Cyber Security Workforce

Dr. Char Sample, & Dr. Connie Justice

Introduction

Cyber Security programs continue to expand across universities creating their own academic silos in response to growing workforce demands for cyber security professionals. Strong industry growth justifies this growth pattern in cyber security programs. These programs continue to turn out specialists that support the market demand.

However, a growing chorus have observed the need to break down silos, and are also calling for cross-disciplined approaches to solving cyber security problems (Peltsverger, 2015; Rowe, Lundt & Eckstrom, 2011; Crowley, 2003). Disciplines such as law, psychology, sociology, resilience, reliability, statistics, data science, international studies and others are becoming increasingly intertwined with cyber security (Ibid). The existent cyber security programs across accredited universities overwhelmingly continue to offer the same courses in penetration testing, policy, reverse engineering, risk, forensics, management and computer/network architecture; thus, Peltsverger's study of 2015 is still very applicable today.

In order to support the growing need for cross-discipline cyber security professionals, accredited cyber security programs will need to update their focus to not only embrace other academic disciplines, but also to understand how those disciplines can contribute to the improvement of cyber security and vice versa. A potential first step in this journey may begin with the offering of a security architecture course, where students are forced to acquire a cursory knowledge of other disciplines in creating a workable security solution.

Traditional architects combine knowledge from various disciplines in order to design structurally sound buildings (Savold, Dagher, Frazier, & McCallam, 2017). Similarly, security architects use skills learned in other disciplines to create robust network security solutions that support organizational goals. Creating strong defensive networks in support of a mission requires a mix of breadth and depth in the skill set of the network architect (Triolo, 2014).

Background

Academia silos exist because expertise is gained through research that focuses on a specific discipline while excluding others. Studies are purposefully tightly

restrained to allow the researcher to focus on a specific problem. Variables are limited, so that results or findings can be generalized for application where the same variables appear in different environments. Thus, cyber security would naturally follow the same structural pattern. This ultimately leads to cyber security professionals who are unable to effectively communicate with other groups in the workplace.

Cyber security programs have responded to industry's demand for skillsets. This approach showed initial successes. However, like nursing where professionals initially took care of patient's immediate needs, programs evolved to include increasing numbers of courses and disciplines (psychology, chemistry, sociology, kinesiology, etc.) in order better prepare nurses for their jobs. So too, cybersecurity curricula must evolve to include other disciplines with the goal of improving the students for the future workplace.

Cyber security is increasingly being asked to support other disciplines (law, finance, psychology, sociology, etc.) yet the programs are not reflecting this in their curricula. This failure to adequately support other disciplines further isolates cyber security professionals and may limit the students to becoming industry commodities. Commodities are quickly picked up and discarded this can be problematic for career growth.

These factors increasingly suggest the need to restructure cyber security programs away from the silo approach and into the cross-disciplined approach. The overall problem facing educational institutions, and students is that accredited programs may not adequately prepare their students for cybersecurity workforce challenges where diverse skill sets are becoming increasingly important. The general problem is the universities are focusing on technical rather than the holistic education of the cybersecurity learner when the workforce has a growing need for the holistic cybersecurity professional (Triolo, 2014).

Proposed Solutions

There are several potential solutions to the cyber security silo problem and each one warrants discussion. The proposed solutions are not limited to those discussed here and are likely highly situational. In some cases, some institutions may find some programs unworkable, for this reason these are suggestions not requirements.

1. Create a liaison position in the departments that interacts with other disciplines. This approach would entail hiring a liaison who reaches out to different

departments and works to define the necessary courses to make cyber security a joint major with the available disciplines.

2. Embed departments together for work on a common goal. An example of this approach occurs at Cardiff University in Wales where criminal justice, cyber security, data science, psychology, computer science exist in teams that work together in solving common research problems.
3. Require cyber security to be a dual major or joint major at the undergraduate level. This would force cyber security students to understand how cyber supports other disciplines and communicate with personnel in a manner that demonstrates an understanding of the discipline..
4. Create distinct curriculum for cybersecurity majors that include, but not limited to; cybersecurity risk assessment, creating policies, third party risk, and network security architecture.
5. Create cybersecurity curriculum for all disciplines to take before taking curricula in specific disciplines. See figure 1. Additionally, we could create common cybersecurity curriculum before discipline specific curriculum and midway or end of discipline specific curriculum, see figure 2.

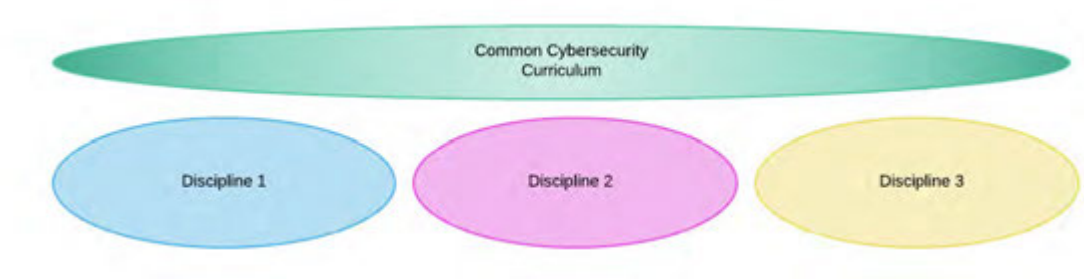


Figure 1: Common cybersecurity curriculum

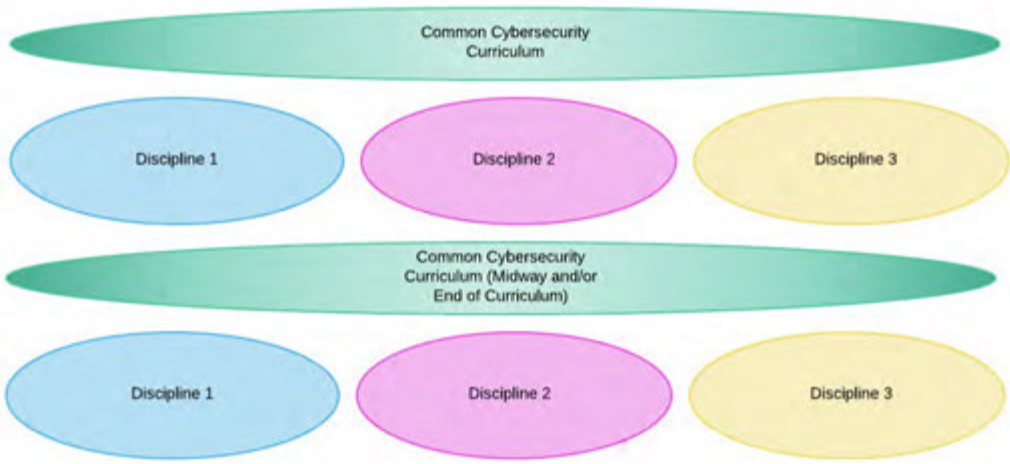


Figure 2: Common cybersecurity curriculum before and midway and/or end of curriculum

Specialized roles such as penetration testers and reverse software engineers provide an entry point into an organization, but generally speaking not professional growth opportunities Triolo (2014) noted that attackers need to be correct once and defenders need to be correct every time. A certain set of skills must bridge the gap between attacker skills and defender skills.

"Security architects design, build and oversees the implementation of network security for an organization" ("Become a security architect", n.d.). The security architect is entrusted to create a solution that reflects a deep technical knowledge of security products, and how to integrate those products in support of organizational goals. Solutions are complex and must work (Ibid). This mix of technical skills, management skills and people skills are unique. Introducing this mix of skills in cyber security programs as a foundational course would provide a foundation for a wider path of experiences for students and a potential bridge for those wishing to focus on policy.

Security professionals are frequently reminded to "bake in" security, not "bolt it on". This security by design must be engineered to the environment and processes that the security solution supports. Designing in security requires other disciplinary knowledge outside of the traditional technical areas.

Many universities and colleges participate in capture the flag cyber challenges that require participants to act as both attackers and defenders (Manson & Pike, 2014). These exercises are primarily focused on vulnerability exploitation, with prevention

being covered as a reaction to attack signatures (Manson & Pike, 2014). In some cases the cyber challenges require teams to build resilient solutions, but once again these solutions are designed to withstand known attacks in general. Creating and building of defences, in this arrangement, becomes an ad-hoc process that lacks rigor.

Conclusion

The changing nature of problems requiring cross-discipline approaches to cyber problems will force change in educational institutions programs. These changes will need to recognize the importance of other academic disciplines in creating the next generation of cyber security professionals. This paper put forth suggestions to offer potential ways forward.

References

Andel, T. R. and J. T. McDonald (2013). A Systems approach to cyber assurance education. *Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference.* Kennesaw GA, USA, ACM**:** 13-19.

Become a security architect. (n.d.). Cyber Degrees. Retrieved from https://www.cyberdegrees.org/jobs/security-architect/

Henry, A.P. (2017). "Mastering the cyber security skills crisis: realigning educational outcomes to industry requirements" ACCS discussion paper no. 4, August 2017, Australian Centre for Cyber Security, UNSW

Canberra, Canberra, viewed 26 Feb 2018, Available: https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/uploads/ACCS-Discussion-Paper-4-Web.pdf

Crowley, E. (2003, October). Information system security curricula development. In Proceedings of the 4th conference on Information technology curriculum (pp. 249-255). ACM.

Joint Task Force on Cybersecurity Education (2017). Cybersecurity Curricula 2017. Available: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Knapp, K. J., et al. (2017). "Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance." Journal of Information Systems Education 28(2): 101-113.

LeClair, J., et al. (2013). An Interdisciplinary Approach to Educating an Effective Cyber Security Workforce. Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference, ACM, (LOCATION).

Peltsverger, S (2015) "A survey of university system of Georgia cyber security programs" , Proceedings o the 2015 Information Security Curriculum,

Manson, D. and R. Pike (2014). "The case for depth in cybersecurity education." ACM Inroads **5**(1): 47-52.

McGettrick, A., et al. (2014). Toward curricular guidelines for cybersecurity. *Proceedings of the 45th ACM technical symposium on Computer science education*. Atlanta, Georgia, USA, ACM**:** 81-82.

Murphy, D. R. and R. H. Murphy (2013). Teaching cybersecurity: Protecting the business environment. *Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference*. Kennesaw GA, USA, ACM**:** 88-93.

NISTIR 8193 (DRAFT), National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators: Indicators for Performing Work Roles. (n.d.). Available: https://csrc.nist.gov/publications/detail/nistir/8193/draft

Ramirez, R. B. (2017). Making cyber security interdisciplinary: recommendations for a novel curriculum and terminology harmonization, Massachusetts Institute of Technology.

Savold, R., Dagher, N., Frazier, P., & McCallam, D. (2017, June). Architecting Cyber Defense: A Survey of the Leading Cyber Reference Architectures and Frameworks. In *Cyber Security and Cloud Computing (CSCloud), 2017 IEEE 4th International Conference* on (pp. 127-138). IEEE.

Triolo citation - https://www.scmagazine.com/hackers-only-need-to-get-it-right-once-we-need-to-get-it-right-every-time/article/537904/

Dr. Connie Justice
Department of Computer Information and Graphics Technology
Purdue School of Engineering and Technology
Indiana University Purdue University Indianapolis
cjustice@iupui.edu
317.278.3830

Dr. Connie Justice has over 30 years' experience in the computer and systems engineering field. Professor Justice is a Certified Information Systems Security Professional, CISSP. She created the networking and security options for CIT majors and a Network Security Certificate Program. She has designed and modified many courses in networking and networking security curriculum. Professor Justice is noted for her creation of the Living Lab, an experiential learning environment where students gain real world experience running an IT business.

Professor Justice takes extreme pride and is a great innovator in the area of experiential learning and service. Professor Justice has published several papers on creating course curriculum for information assurance and security. Professor Justice enjoys connecting students with industry projects that can provide them much needed hands-on experience.

Dr. Justice consults for and has managed IT departments in small, medium, and large sized businesses. She serves as Senior Security Advisor for a fortune 100 company. Her areas of research include: experiential and service learning, information and security risk assessment, risk management, digital forensics, network security, network and systems engineering, network and systems administration, and networking and security course development.

Dr. Char Sample

Dr. Char Sample is research fellow employed for ICF International at the US Army Research Laboratory in Adelphi, Maryland, and is also with the University of Warwick, Coventry, UK. Dr. Sample has over 20 years experience in the information security industry. Most recently Dr. Sample has been advancing the research into the role of national culture in cyber security events. Presently Dr. Sample is continuing research on modeling cyber behaviors by culture, other areas of research are information weaponization, data fidelity, and deceptive data.

Stephanie Siteman
Facebook InfoSec Diversity & Academia Program Manager
Proposal NACE

Stephanie Siteman is currently a manager at Facebook on the Cybersecurity Team. She handles all diversity and education initiative's that include curriculum, conferences, and direct relationships with education providers. She manages both domestic and global outreach projects and programs. She recently spoke at F8 about how to increase diversity in the workforce. She is passionate about making impact for the students, professors and universities.

1. What do we need to educate the next generation of cybersecurity & privacy specializes?
    a. We need to do a better job of bridging the gap between industry and academia by working closer together and learning from each other
    b. We need more quality hands on cybersec education available to the majority
    c. We need easier access to trainings and workshops and conferences
    d. We need diverse leaders and educators
    e. Change the way we think of cybersec
    f. Flexibility
    g. Sharing more best practices
2. How do we attract and educate a diverse set of students to succeed in a variety of national and private sector positions?
    a. Get leaders from both sectors to fully care and commit
    b. We need to make a clear and purpose effort
    c. We need to think differently
    d. We need to work with schools in the elementary schools and up
    e. We need to work with parents
    f. Diverse role models
3. What are some good ways to "future-proof" the education we provide?
    a. Plan to have the education dynamic and be flexible since security is ever-changing
    b. Create a roadmap and model as a foundation
    c. Find people who care and stick with them

Broadening and Diversifying the Reach of Cybersecurity Education

Abhilasha Bhargav-Spantzel, Principal Engineer, Intel Corporation
David Bills, Director of Academic Programs, Intel Corporation

Cybersecurity education is of prime importance in today's world. Increasing threats from attackers are motivated by financial and other gains, and these bad actors have access to advanced tools, resources and services from the hacker community.

This growing problem is evident in numerous news reports on the impact of cyber-attacks on individuals and organizations across the globe, and it will only get trickier as more digital devices and services become available in the future. These challenges, coupled with the shrinking talent base of solutions expertise, highlight the importance of broader cybersecurity education.

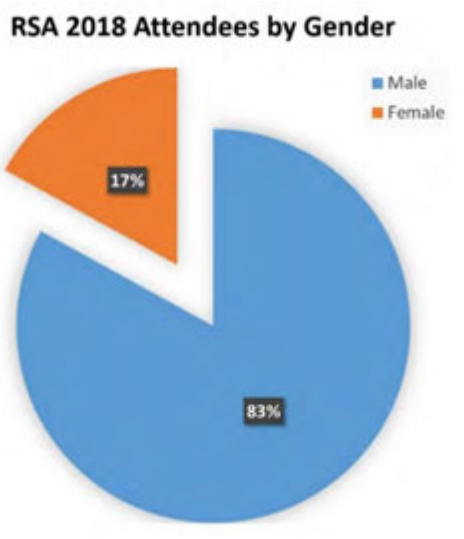
We need a comprehensive and granular approach. While no single individual is an expert in all cybersecurity areas, **foundational elements** can help provide the needed professional skills. This foundation should foster deep knowledge of the history and origins of cybersecurity challenges and solutions, as well as a good **understanding of their diverse range and interdisciplinary relevance**.

For decades, we've seen **significant research and security assurance initiatives**—from the U.S. Department of Defense Orange Book in the 1980's to the European Union's General Data Protection Regulation (GDPR) today. These efforts point to the network security protocols, system security design principles, privacy enhancing technologies, threat modeling, and other foundational elements for cybersecurity education. These must be coupled with an understanding of **today's compute platform**, not only **PCs** and **cloud** servers, but also internet of things (**IoT**) devices, connected **cars**, and the **ever-evolving world of digital services**.

This broader education effort must be grounded in how cybersecurity impacts us in both the **cyber and physical world**. The corresponding importance of **safety, privacy** and the **long-term consequences** to individuals and to society must also be considered.

To develop such a comprehensive approach, we need to nurture a diverse group of individuals—both teachers and students—to motivate and strengthen the defenses that become part of the design in every engineer's respective field. There is **no one-size-fits-all to attract the diverse set of individuals,** so one must **employ targeted tactics to attract** specific groups of **individuals.**

The lack of diversity evident at RSA-2018, where women comprised only 17 percent of attendees, points to a problem that needs to be tackled**. "Failure of imagination**" has been cited as the reason we were caught off-guard by the Russian interference with the 2016 U.S. presidential election, and the same was said about Sept. 11, 2001. By bringing more types of



people with a more diverse range of experiences and backgrounds into protecting our security, we can broaden the imagination brought to bear on future threats, especially in the cybersecurity domain.

We as society have yet to understand the full impact and cost of decisions made yesterday, today regarding **privacy**. We must think this through completely and how it will **impact our future** and the future of generations to come. If we are not careful, we will see our **technologies weaponized** which makes nuclear warfare obsolete. A scary proposition!

Finally we need to **future proof** our education system. The **education system** has never moved at the **speed of technology** and business and this must change. Education must have **a sense of urgency** and move at a faster pace. As part of growth mindset – we need to get out of the old mentality of how school is run. One way is to **partner with industry** to understand the pain points and quickly **develop the curriculum to bridge the gap**. **Education meets real-world experience and moves at the speed of business**. This has to be tackled carefully to **avoid "shiny object syndrome"** and ensure the due diligence is done to tackle the underlying problem. The education goes both ways, similar to many feedback loops in carefully designed security and risk management systems to allow continuous education opportunities for all.

It is great to see strong cybersecurity education efforts by notable leaders academia, government and industry. For example, Intel is leading initiatives with the academic community to bring diversity to high-tech in general and cybersecurity in particular. We focus on **outreach programs** to universities and students of **all genders, backgrounds, interests** and various majors to talk about the comprehensive cyber security considerations.

Training cybersecurity professionals is now more critical than ever. A recent government and industry Task Force is predicting that 1.8 million cybersecurity-related positions worldwide will go unfilled by the year 2022. Building collaborative programs and ensuring diversity of representation in these programs would be critical in **addressing this shortfall** in needed professionals to tackle the challenges and **win on our path ahead.**

Abhilasha Bhargav-Spantzel is an Intel Principal Engineer focused on identity, security and privacy. She has numerous patents and broad experience in identity management, cryptography, biometrics, hardware devices and system security. She leads multiple diversity and inclusion efforts at Intel, and actively drives development of women in engineering and cyber security. Find her on LinkedIn.

David Bills is the Director of Academic Programs for the Platform Security Division where he collaborates with academia to drive security research, education, and talent acquisition. For the past 2 years, he has served on Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS) board. David built Intel's scale ISV software enabling ecosystem from prior to his academic work. LinkedIn

The need for a National Cyber Academy:
The United States Cybersecurity Academy

In the 21st century, the landscape for war has extended from land, sea, air, and space to a fifth domain- cyberspace. America's digital strategic infrastructure is now considered a "strategic national asset" and protecting this has become a national priority. The state of cybersecurity for the nation has reached a critical status. There is an urgent need for skilled cybersecurity professionals across the workforce and for leaders in the federal government, across the security agencies. The National Science Foundation's Scholarship for Service program is one vehicle geared towards encouraging the best cyber talent to work for the government, at least for several years, before being lured to industry for higher salaries. This program has encouraged many students to work for agencies such as NSA, CIA, etc.

The cybersecurity crisis requires a multifaceted solution and the time is right for another service academy focused in cyber. Dr. Mark Hagerott and Admiral (Ret.) James Stravridis formally recommended this in March 2017 in their Foreign Policy article entitled "Trump's Big Defense Buildup Should Include a National Cyber Academy." Additionally, Dark et al. propose the idea in the 2018 CISSE paper entitled: The Cyber Cube: A Multifaceted Approach for a Living Cybersecurity Curriculum Library.

There is a history for this. After the Revolutionary War, soldiers and legislators, including Washington, Hamilton and John Adams, concerned about American reliance on foreign engineers and artillerists, lobbied for the creation of an institution devoted to the arts and sciences of warfare. In 1802, Thomas Jefferson signed legislation to establish the United States Military Academy at West Point, a strategic military center. In addition to providing military officers, the USMA became the first accredited civil engineering school and its early graduates helped construct the nation's first railway lines, bridges, harbors and roads. The mission of the USMA is: "To educate, train, and inspire the Corps of Cadets so that each graduate is a commissioned leader of character committed to the values of Duty, Honor, Country and prepared for a career of professional excellence and service to the Nation as an officer in the United States Army."

Similarly, the United States Naval Academy was founded in 1845 in response to a need for trained officers at sea. The curriculum of the USNA has shifted to accommodate the high tech fleet of nuclear-powered submarines and surface ships and supersonic aircraft .The USNA, located in Annapolis, MD, states the following mission – "To develop Midshipmen morally, mentally and physically and to imbue them with the highest ideals of duty, honor and loyalty in order to graduate leaders who are dedicated to a career of naval service and have potential for future development in mind and character to assume the highest responsibilities of command, citizenship and government."

Most recently, the Air Force academy was built to address our needs in aerospace including missiles and atomic weapons. Following decades of political pressure to increase America's air power, it was not until 1954 that President Eisenhower (ATC) initiated a detailed curriculum for the Academy program. The United States Air Force (USAF), formed as a separate branch of the U.S. Armed Forces in 1947, is the aerial and space warfare service branch of the United States Armed Forces. The Air Force defines its core missions as "air and space superiority, global integrated ISR, rapid global mobility, global strike, and command and control." While each of the military academies have their own cyber programs, their primary aim is to provide officers to their respective military branch. The numbers are relatively small - the USMA produces 15 graduates per year and the USNA's freshmen class has 110 cyber operations majors (the class of 2018 had 22 cyber majors). While some service academy graduates eventually work for the federal agencies, generally this is after they have completed their service requirements.

The defense and military landscape has changed, and the nation's infrastructure and public safety are at stake. The United Stated Cybersecurity Academy (USCA) that produces the much-needed cyber specialists for the federal government would bolster the status of the US in the international arena and help protect our critical infrastructure. Additionally, the USCA would provide a center or hub for the cybersecurity community and foster synergistic activities, such as workshops, training, lectures, competitions and other cyber events, to vitalize national workforce development.

The USCA would in many ways resemble the existing academies, accredited, free, and selective, but graduates would be required to serve as civil servants for the federal government. The cybersecurity major could resemble the NSA cyber Ops program, be deeply technical, and include computer science, cybersecurity offense and defensive skills as well as a solid liberal arts courses including history, government, and cyber laws. Given the technical landscape, the USCA

should be adaptive and include significant virtual infrastructure to allow cybersecurity leaders and experts across the world to provide instruction remotely. The faculty of the USCA would not be tied to the traditional doctoral requirement as for most four-year schools, but instead facilitate the cybersecurity experts in the country to serve as faculty. Additionally, the entrance requirements would allow for students with disabilities. A prep school or ROTC program geared towards cyber would be a good complement, perhaps following a model as being kicked off in Huntsville Alabama.

Obviously, the costs for such a brick and mortar institute are high, so I propose that the academy begin as a virtual infrastructure, including a "national credit" model where the USCA offers full courses in critical areas such as reverse engineering and cyber operations. National credit would allow schools that are trying to build cyber programs supplement their programs by accepting the USCA courses for credit. The academy should include a library of cybersecurity resources for K-20, including curriculum that is mapped to national standards and aligned to learning taxonomies, including labs and exercises and different modes of instruction. Additionally, a cyber range, both public and private, is necessary to support the academy and the digital library. Given the national shortage of cybersecurity faculty, this would help better prepare the cyber workforce.

In addition to start-up and operating costs, another significant challenge to a national cybersecurity academy is diversity. Since women were permitted to enter the military academies in 1975, each of the academies have worked hard to achieve diversity and each has struggled against perceptions of hostile environments. The USCA must be created with an eye towards fostering diversity, not only for women but across ethnicity, to provide an inclusive environment. Socialization and courses on inclusion and acceptance would be key to producing cyber leaders with these attributes.

Cyberspace is the new battlefield. It is imperative that the United States prepare for it on all fronts.

Luis M Vicente
Associate Professor, Associate Director,
(ECECS) Electrical, Computer Engineering and Computer Science Department,
Polytechnic University of Puerto Rico (PUPR)
377 Ponce de León Ave, Hato Rey, PR 00918
(787) 622-8000 Ext. (340) / Fax: (787) 281-8342

Personal address:
131 Calle Portugués, San Juan, PR 00926
lvicente@pupr.edu ,1-787-217-4563

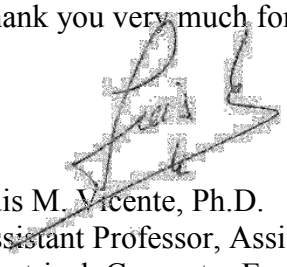
Dear organizers of the 2018 NACE Workshop,

This is Luis Vicente, faculty member of the Polytechnic University of Puerto Rico (PUPR). I am writing you this letter because I would like to participate in the NACE Workshop, on June 9-10, 2018 in New Orleans, LA. PUPR is a National Center of Academic Excellence in Information Assurance Education (CAE/IAE) and we are devoted to graduate students proficient in Cybersecurity among other fields.

I am part of the PUPR faculty as Associate Professor, Associate Director of the ECECS Department. My main interest attending this workshop is to learn about new Cybersecurity trends, how to efficiently teaching these topics to our students. Also, find about funding, educational, and professional opportunities for our Hispanic students in Puerto Rico. Here at the PUPR most of our faculty and almost 100% of the students are from Hispanic minorities. However, since Puerto Rico is a US territory we all hold US citizenship. This put our students in a very advantageous potential position of being able to work anywhere in the USA, including classified jobs. Last but not least, I would like to increase the underrepresented Hispanic group in the Cybersecurity and National Security fields. The reality is that our minority is not fully represented in those areas yet.

Please find attached a short bio sketch, and a paper intended to inspire thought and discussion about the field of Cybersecurity.

Thank you very much for your attention.



Luis M. Vicente, Ph.D.
Assistant Professor, Assistant Director ,
Electrical, Computer Engineering and Computer Science Department,
Polytechnic University of Puerto Rico,
377 Ponce de León Ave, Hato Rey, PR 00918
(787) 622-8000 ext (340) / Fax: (787) 281-8342 / lvicente@pupr.edu

Dr. Luis M Vicente is the associate director and associate professor of the Electrical & Computer Engineering and Computer Science Department at the Polytechnic University of Puerto Rico. He received Ph.D. in Electrical and Computer Engineering at the University of Missouri-Columbia in May 2009 where he already was author or coauthor of five publications.

From February 1990 to February 2003, Dr. Vicente worked in industry. First, in the Military-Aerospace Division, SENER Group, Spain. In addition, he worked with Voyetra Inc., New York, and with SIEMENS Corp., Madrid.

From February 2003 to June 2009, he became Assistant Professor at the Polytechnic University of Puerto Rico (PUPR). In 2009, Dr. Vicente was promoted to Associate Professor and Mentor of the Master Program in Electrical Engineering at the PUPR. In 2011, he was appointed Sponsor Research Office Coordinator.

In 2012, he was promoted to Associate Director. His research interests include beamforming, array processing, statistical signal processing, adaptive filters, High Performance Computing on Signal processing, and Cybersecurity. As a graduate thesis advisor, he already graduated fifteen students in the digital signal processing area, high performance computing and parallel processing. He is now pursuing a Graduate Certificate in Digital Forensics, expecting to be completed in fall 2018.

Cybersecurity permeates all aspects of our society. It is well known that every electronic equipment connected to the web is susceptible to be hacked, spied on, and the probability of that happening is almost one hundred percent. If that is so, why people are still in negation? What is the reason Cybersecurity is not already part of elementary courses in Engineering? Or even more, why is not taught in every high school in our country, at least at the basic level?. It seems we only pay attention to Cybersecurity after we have been victim of a cyber-crime. We need to change that into a proactive measure!!

The first measure to arm ourselves against cyber-crimes is to be aware of its reality. Learn the basics and at least have a true knowledge of what are the risks we are taking when going online. Getting involved in Cybersecurity is not difficult at all. To have a basic knowledge of how viruses work, how to protect ones computer and smartphones could be learned for people with less than high school academic level. Almost every one of us know what is an anti-virus, a virus, have some ideas of Trojan horses and such. However, all this knowledge usually comes to us from not verifiable sources, like Facebook, personal blogs, unverifiable web pages, gossip. It would not be better to acquire this knowledge from verifiable, academic sources? Why not be learned in schools by adequate teachers in the area? Why not learn all the topics in their correct order and with a strategy in mind? These concepts do not require advanced mathematical skills. These advanced mathematical skill are only needed if you really want to have a deep knowledge of some areas, for example, in cryptography.

Recently, some universities are paying more attention to the importance of Cybersecurity, and not only Engineering universities, but also universities devoted to law. From Chuck Easttom book Computer Security Fundamentals, we read that the University of Dayton School of Law has an entire website dedicated to cyber-crime. The university has extensive links on cyber-crime, cyber stalking, and other web-based crimes. As we all move forward into the twenty-first century, we should expect to see more law schools with courses dedicated to cyber-crime.

I propose to encourage the teaching of some basic topics in Cybersecurity at the very high school level, or even earlier. Starting with the concept of networking layers. To have at least the awareness that all our communications are structured in OSI layers. Then, teaching the students how the

hackers use these layers to infect the network with malware. In addition, a basic knowledge of all kind of malware should be part of the class. The difference between virus, worms, Trojan horses, among other. In addition, chapters on anti-virus, firewalls, anti spyware, would be needed to have a global idea of the basics of Cybersecurity.

None of the above would permeate the mind of our young students without some hands-on laboratories. I propose the creation of some basic laboratories where the students could implement and connect a small network. Both wired and wireless. To acquire the basic knowledge of how it works and how the devices communicate with each other. In addition, some testing, penetration testing, and vulnerability testing. All inside a controlled laboratory network of computers. Create contests where some students would be the defensive barrier of a network and other students to be the cyber attackers.

One of the main difficulties in making reality above ideas is the assumption that all knowledge acquired by our young students could be used for criminal purposes. I am against that idea when referring to our American joung students of at least 16 years old. Let's think for a moment what is the minimum age for americans to use and practice with a long shot gun. Just a look at a Washington Post article (By Roberto A. Ferdman and Christopher Ingraham August 27, 2014), we learned that in 30 states there is no minimum age. To me it does not seem a great idea to give a gun to a children, but if we think of young students, around 16 years old. Should we prohibit the knowledge of guns because they could be potential criminals? It is not true that they could learn the topic form the internet, and not precisely by the best people to teach how to use, and the risk of using them? Let's make another analogy. Sex. Why is necessary to teach youngsters about sex? We all know why. However, sex has been a taboo for centuries. Nobody would want to talk or even teach about it. Now, what is the trend today about sex? Why it should be different with Cybersecurity? It is not better to teach all aspects of Cybersecurity in our controlled schools, to young people of at least certain age, than for them to learn from real criminal hackers posting tutorials in the web, and performing penetration testing on the neighbor Wi-fi access point?

We know in conferences and workshops when the speaker ask if your company has been hacked, not everybody wants to disclose that. It seems is shameful to be a victim of cyber-crime. Not

everybody wants to admit they have been victims of a cyber-crime. Cybersecurity is our present time taboo. However, we know by experience in other areas of our life that is better to have good basic knowledge of certain topic than to ignore it or even learn it from the wrong teaching channels. We need a paradigm change in order to place Cybersecurity in its own level of importance.With the fast trend of newer technologies, even faster than ever, we have to admit that the level of importance is rather high. We need to be prepared, armed and ready to know, and defend ourselves against the risks of using technology. We need to prepare our American students to join the good guys.

Regarding the question of how do we get more US citizens, and a more diverse population, into cybersecurity in meaningful ways? I could answer this from our little Caribbean island of Puerto Rico. From centuries, this has been a land of pirates, buccaneers, and smugglers. Even today, the black market, narco-activity, violent crime on our small island streets is rampaging. There is not a single family in the island where that kind of violence did not touch in one or another aspect. On one hand, it is not difficult to convince our young people to join the bad boys, fast money, fast life, short life. However, here in our universities, we are given them sanctuary and teaching them to arm themselves against that kind of life. We teach them how to outsmart the bad people using the latest technology available. We give them power. As I stated in my presentation letter, PUPR is a National Center of Academic Excellence in Information Assurance Education (CAE/IAE) and we are devoted to graduate students proficient in Cybersecurity among other fields. This is a challenge that any smart student would take, making them truly heroes!!. To outsmart the bad people and to contribute the goodness in this island is something not easily understood for people that did not suffer the violence of our streets. For young Puerto Rican students that have seen real suffering, to become proficient in an area where they feel they can contribute to goodness is a true mission. Most of our graduated students are working for security agencies in Washington. They are proud and they make us proud. We have more motives to anyone to help our young students from the beginning of their academic life to learn Cybersecurity. And, we are committed to do so.

Take a Long View: Integrate Security Topics into ALL Software Development Education

The software development community does a lousy job of delivering software that minimizes the attack surface. In the National Vulnerability Database [8], an exact match search on the keyword Microsoft identifies 275 records for the last 3 months. A similar search on the keywords Linux and Oracle identifies 218 and 326 records, respectively, for the last 3 months. Neither proprietary nor open source software are immune from bad or ignorant secure software development practices. This situation is not new. In the SANS report on the Top 25 Software Errors [10], the current list identifies 16 errors that also appeared in the 2010 list.

Our current state of ineptitude is even more perplexing when one considers that two researchers published eight security principles in 1975 [9], over forty years ago! Five more security principles were described in 2013 [7]. Why aren't these thirteen security principles - economy of mechanism, fail-safe defaults, complete mediation, open design, separation of privilege, least privilege, least common mechanism, psychological acceptability, secure the weakest link, defend in depth, be reluctant to trust, promote privacy, and use your resources – discussed and practiced in all undergraduate curricula that has a role in software development?

There appears to be some positive momentum in emphasizing secure software development in undergraduate computing programs.

The most recent computer science undergraduate curriculum guidelines (CS2013) represents the first time security was recognized as a separate knowledge area with the inclusion of Information Assurance and Security [1]. The most recent software engineering and information systems undergraduate curriculum guidelines - SE2014 and IS2010, respectively - have significantly increased the visibility of security.

The current CISO of Turner Broadcasting System is calling for a “moonshot to reestablish our digital strength (via) a profound, coordinated effort to bolster our cybersecurity systems and protect our democracy from hackers” [3]. In his book, Chronis draws inspiration and lessons learned from other moonshots – getting a man on the moon, defeating fascism, and eradicating polio. One of his pillars for fixing cybersecurity is to minimize software vulnerabilities through better software development practices, market incentives that provide more information to consumers about the safety and security of products, and software

technologies that make it easier to identify/fix security defects (e.g., self-healing code, deep learning platforms).

It is clear that both educators and industry see the need for vast improvements in how we develop software. The question becomes, how do we cover security topics in our computing-based programs so that we have the greatest impact on the next generation of information technology leaders? While this question pertains to the three curriculum guidelines (CS2013, SE2014, and IS2010) most directly related to software development, only the CS2013 perspective is described below.

One option is to create a separate computer science course that covers cybersecurity. Assuming CS programs make this course a requirement and not an elective; this would likely improve students understanding of security topics and their use in software development. Another option is to integrate security topics into the entire CS program. This is what we have done in our INCUBATE project [4, 11]. One example of this integration is in our CS1 course, where we introduce security principles (e.g., CIA, anonymity, authentication, assurance, and non-repudiation) and input validation, with hands-on exercises that ask students to apply various types of input validation checks. While our assessment results to-date are positive, our first cohort of students that will have experienced four years of integrating cybersecurity topics into CS will graduate in May 2019. While we expect assessment results to be positive for this cohort, the full impact of our efforts will be unknown for at least another 5-10 years, or until these students have gained enough work experience to influence the culture within their respective organizations.

Changing the culture of the software development industry to adhere to security policies and to apply security controls and mechanisms will take time. Perhaps twenty years from now, when current college students start to take on leadership positions, we will see results of the educational decisions we make over the next few years.

Diversity of Thought: Social and Political Perspectives on Cybersecurity

Since technology has created our cybersecurity problems, technology can solve these problems. This thinking is shortsighted because it ignores the fact that humans develop and use these technologies, and humans are the source and target of cybersecurity attacks.

Having students study the social sciences as part of a cybersecurity program provides these students with other ways of thinking about the issues that confront us. A workshop on social science, computer science, and cybersecurity held in 2013 [5] had as its goal to develop communities of researchers from social science and technology fields that cooperate in the development of new and improved cybersecurity systems. In the summary report from this workshop [5], white papers written by the attendees provide their perspective on the workshop goal. The following quote exemplifies the workshop discussions in support of the need for educational opportunities that blend social sciences and information & system security technology.

> "The fact that humans from several different walks of life are interacting with these systems on a daily basis has prompted a paradigm shift: rather than designing secure systems with arbitrarily defined use models, we must design secure systems with use models informed by how people interact with each other, computers, and information. This security paradigm necessitates a close collaboration between technical and social scientists so that the design of secure systems incorporates an understanding of the needs and capabilities of the billions of people that will rely on them." (Page 28, Chris Kanich, Computer Science Department, University of Illinois at Chicago.)

In addition, a 2014 paper published by the National Council in the Social Studies [2] includes the following quote.

> "… the disciplines of the social sciences promote ways of knowing and deliberating about data and information that are critical to policy development and the implementation of cybersecurity initiatives. Building the capacity of the next generation of social scientists to tackle these emerging issues is imperative."

While Chronis [3] believes that minimizing software vulnerabilities is crucial to his cybersecurity moonshot, the other pillars of his moonshot relate to social and political perspectives. His other pillars: educating everyone about social engineering attacks; federal government leadership in the form of regulations and incentives; and better corporate governance of their cybersecurity programs.

Le Moyne College launched a new cybersecurity undergraduate program in fall, 2017 developed by faculty in anthropology, computer science, criminology, political science, and sociology [6]. This program has used the Catholic Jesuit mission of *educating the whole person* as motivation for *educating the whole cybersecurity professional* with perspectives in: crime, society & culture; information & system security; and policy & law. Our thinking in developing this new program is to position our students for success in a variety of career paths, some of which may have an ancillary relationship to cybersecurity.

Bio Sketch

David Voorhees is an associate professor of computer science at Le Moyne College. He is the director of the computer science, software applications and systems development (i.e., a software engineering program), and cybersecurity undergraduate programs. Dave worked for 19 years in industry before starting as a visiting assistant professor at Le Moyne in August 1999. He earned his Ph.D. in computer science from Nova Southeastern University in 2005. Dave is the PI of the NSF-funded INCUBATE project briefly described in this paper.

References

[1] ACM, (2018). *Curricula Recommendations*. Retrieved April 29, 2018 from https://www.acm.org/education/curricula-recommendations.

[2] Berson, M. J., & Berson, I. R. (2014). Bringing the Cybersecurity Challenge to the Social Studies Classroom. *Social Education (National Council for the Social Studies), 78(2), 96-100*.

[3] Chronis, P.K. (2017). *The Cyber Conundrum: How do we Fix Cybersecurity?.* CreateSpace Independent Publishing Platform.

[4] Das, A., Voorhees, D., and Choi, C. (2018). *INCUBATE: Injecting and assessing cybersecurity education with little internal subject matter expertise*. Retrieved April 29, 2018 from http://research.lemoyne.edu/incubate.

[5] Hofman, L. J. (2013). Social Science, Computer Science, and Cybersecurity, Workshop Summary Report. Cyber Security Policy and Research Institute, The George Washington University, Report GW-CSPRI-2013-02 retrieved on October 21, 2016 from https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/Final+08+22+13+1301+Report+Social+Science.pdf.

[6] Le Moyne College Catalog, (2018). *New Cybersecurity Undergraduate Program*. Retrieved April 29, 2018 from http://collegecatalog.lemoyne.edu/arts-sciences/cybersecurity/.

[7] McGraw, G. (2013). *Thirteen principles to ensure enterprise system security*. Retrieved on July 28, 2015 from searchsecurity.techtarget.com/opinion/Thirteen-principles-to-ensure-enterprise-system-security.

[8] NIST, (2018). *National Vulnerability Database*. Retrieved April 29, 2018 from https://nvd.nist.gov/vuln/search.

[9] Saltzer, J.H. and Schroeder, M.D. (1975). The Protection of Information in Computer Systems. In *Proceedings of the IEEE, 63(9)*.

[10] SANS, (2018). *CWE/SANS Top 25 Most Dangerous Software Errors*. Retrieved April 29, 2018 from https://www.sans.org/top25-software-errors/archive/2010.

[11] Voorhees, D. and Das, A. (2018). Injecting cybersecurity into a CS program: a non-specialist perspective. *Journal of Computing Sciences in Colleges, 33(6)*.

Junior Cyber Corps

Introduction

Cybersecurity is critical to the national security and economic prosperity of the U.S. By many accounts, there is a severe shortage of trained cybersecurity professionals to meet the current demand in industry, academia, and government. Cyberseek.org currently estimates the shortage at 285,000. Other studies provide estimates that range far higher. These estimates also assume a minimum of a 2 year degree in cybersecurity, a four year technical degree with a cybersecurity focus, and/or cybersecurity certifications such as CISSP, Certified Ethical Hacker, and Security+ to name a few.

Colleges, universities, and other post-secondary education can't solve the problem alone. They are already serving as many applicants as they can and the need for additional faculty at these levels is now becoming a demand. There are programs in place to grow the post-secondary education capacity. Yet even these measure are not projected to meet the growing demands of employers. As this new capability comes online, it is not clear there will be enough interested and qualified students to make effective use of it, thus creating a likely shortage of students applying to participate in cybersecurity programs at the post-secondary level.

We have both an absolute shortage of students applying, and few of those applying are as prepared as they could be with minimal involvement from primary and secondary educators. We need more students interested in and prepared to pursue post-secondary education in cybersecurity.

To address this shortage will require primary and secondary school students to be more knowledgeable about cybersecurity principles and about the wide variety of career opportunities in cybersecurity. We propose a combination of in-school and

extracurricular activities similar to a Junior Reserve Officer Training Corps (JROTC), named something like Junior Cyber Corps.

Junior Cyber Corps

A junior cyber corps is proposed to introduce primary and secondary school students to the field of cybersecurity, as it applies across the many disciplines that it touches (e.g., ethics. law, business, IT, computer science, engineering) and the “soft skills” (e.g. communication skills, people skills, leadership skills). The junior cyber corps will not only introduce foundational knowledge as it relates to these disciplines, but will also introduce students to the career opportunities that exist, along with the pathways that are available to them to take towards these careers.

Such programs could vary in intensity from extracurricular clubs to significant components of a military school or many points in-between. Such variety could require as little as a STEM-capable member of the community willing to volunteer to be a club mentor or a teacher taking on coach-like responsibilities, all the way up to a dedicated staff supporting an entire curriculum.

The cyber corps programs would include in-school classes, after school clubs, competition teams, seminars/tutorials/conferences, and mentoring from cybersecurity professionals.

-- National Cryptologic School, College of Cyber

Encouraging Primary & Secondary School Teachers

Introduction

Cybersecurity is critical to the national security and economic prosperity of the U.S. By many accounts, there is a severe shortage of trained cybersecurity professionals to meet the current demand in industry, academia, and government. Cyberseek.org currently estimates the shortage at 285,000. Other studies provide estimates that range far higher. These estimates also assume a minimum of a 2 year degree in cybersecurity, a four year technical degree with a cybersecurity focus, and/or cybersecurity certifications such as CISSP, Certified Ethical Hacker, and Security+ to name a few.

Colleges, universities, and other post-secondary education can't solve the problem alone. They are already serving as many applicants as they can and the need for additional faculty at these levels is now becoming a demand. There are programs in place to grow the post-secondary education capacity. Yet even these measure are not projected to meet the growing demands of employers. As this new capability comes online, it is not clear there will be enough interested and qualified students to make effective use of it, thus creating a likely shortage of qualified students applying to participate in cybersecurity programs at the post-secondary level.

We have both an absolute shortage of students applying, and few of those applying are as prepared as they could be if there were but minimal involvement from primary and secondary educators. We need more students interested in, and prepared to pursue, post-secondary education in cybersecurity. This can only be accomplished by their teachers introducing them to cybersecurity concepts prior to post-secondary school.

To address this shortage will require primary and secondary school teachers to be more knowledgeable about cybersecurity and career opportunities in cybersecurity. We propose a multi-pronged approach:

1. Increase the cybersecurity resources available to teachers during their college experience as well as part of their continuing professional development.

2. Provide incentives for teachers to gain cybersecurity expertise and share it with their colleagues and students.

Increased Cybersecurity Teaching Resources

Teacher education programs need access to better materials and subject matter experts in order to provide new and existing teachers with the cybersecurity knowledge they need. We believe that a grant program which brings Education departments together with Computer Science/Computer Engineering departments for the purposes of creating and sharing materials for new and existing teachers is needed. Further these same teams should be encouraged to develop materials the teachers can use (and other existing teachers can use) in their primary and secondary school classrooms.

Quality and effective cybersecurity teaching resources developed with these grants should be made available to all primary and secondary educators via a mechanism such as a digital library. Keys to a successful digital library include: being easily accessible, a broad collection of quality and effective materials, robust search capabilities, and continual maintenance of materials and the library itself. While such a digital library should not be run by the federal government, the creation and maintenance of such a library could be seeded with an investment from the federal government.

Further, since the most effective learning often takes place through hand-on experiences, many schools with only rudimentary computer support would benefit from access to a remote virtual training environment or laboratory. While such a training environment should not be run by the federal government, the creation and maintenance could be seeded with an investment from the federal government.

Simply educating new teachers while they are in college is not sufficient. First, this would only reach new teachers and thus greatly limit the growth of informed teachers. Second, the rate of change in cyber security requires refreshing teachers after a few years. Thus, much of the cybersecurity material developed above must also be suitable for use in professional development environments in which existing teachers regularly participate outside of the university or college. Therefore, we recommend the above grant program include grants to create and maintain certificate and badging programs consistent with state guidelines for continuing teacher education and licensing.

Teacher Incentives

The demands upon primary and secondary school teachers is already extraordinary. Simply adding to their to-do list with additional tasks or giving them additional cybersecurity choices will not be enough to achieve the level of engagement that is required. Incentives aimed at individual teachers will be needed. Such incentives should reward both cybersecurity learning as well as passing on that learning to colleagues and students. Possible incentives may include:

- Subsidizing student tuition for cybersecurity-related courses in an Education program in order to make such electives more attractive
- Expanding the Scholarship for Service program to include teachers graduating with a cybersecurity certificate
- Creating free or low-cost cybersecurity-related professional development opportunities for existing teachers

- Forgiving portions of student loans for teachers that achieve cybersecurity-related achievements (e.g., coach winning Cyber Patriot team; earn cybersecurity-related certifications; winning competitive award for cybersecurity-related activities; running successful, cybersecurity-related professional development event in their school)
- Providing tax incentives for companies that offer paid summer positions, like internships, in cybersecurity-related jobs designed for teachers, to give them both deeper cybersecurity knowledge and, more importantly, information on careers in cybersecurity to share with their students.
- Encouraging federal government agencies and departments to offer paid summer positions, like internships, in cybersecurity-related jobs designed for teachers, to give them both deeper cybersecurity knowledge and, more importantly, information on careers in cybersecurity to share with their students.

Conclusion

We face a critical shortage of trained cybersecurity professionals. This shortage is affecting both government and the private sector. The demand for these professionals is growing much faster than the nation's capacity to train new professionals. To date, our efforts to address the problem have focused upon post-secondary and workplace training. These programs will run short of qualified entrants if we don't include primary and secondary school in the solution and that begins with developing a cadre of informed teachers in those schools. The federal government must invest its resources in this community.

-- National Cryptologic School, College of Cyber

CS4A: A New Approach for Cybersecurity Workforce Development

Yong Wang
Beacom College of Computer and Cyber Sciences
Dakota State University
Madison, SD
yong.wang@dsu.edu

Abstract

The paper proposes a new approach, Cybersecurity for All (CS4A), to resolve the cybersecurity workforce shortage challenge. CS4A aims to establish new pathways for nontraditional computer and information sciences and lifelong learners to become cybersecurity professionals through continuing education. CS4A addresses the challenge in three steps: identify cybersecurity skills needed to succeed in cybersecurity, create cybersecurity skill stacks to establish pathways to cybersecurity career, and develop flexible and accessible cybersecurity programs for people of all ages. In addition to the current endeavors from government, academia, and industry, CS4A reaches, recruits, and prepares a new talent pool of candidates for cybersecurity workforce and thus help resolve the cybersecurity workforce shortage challenge.

I. Introduction

The cyber threat landscape has changed over in the last 20 years. Cyberattacks are surging and becoming more organized and structured. The technology and tactics used by cyber criminals also become more complicated. The sophistication has outpaced the ability of IT and security professionals to address the threats (Cisco 2015). As a result, data breaches are getting bigger. In a recent data breach in Equifax in 2017, 143 million Americans' sensitive personal information was exposed (FTC 2017). Cybersecurity is a national priority (The White House 2017). However, finding qualified people to help drive successful cybersecurity programs has become a nontrivial task. Cybersecurity skills shortage has become a top challenge for organizations in the world (Suby & Dickson 2015). The 2017 Global Information Workforce Study estimates that the cybersecurity workforce gap will reach 1.8 million by 2022 (Center for Cyber Safety and Education 2017). While government, academia, and industry have worked together to address the cybersecurity skills shortage, it is apparent that more efforts are needed to fill the gap as the data reveals that the cybersecurity skills gap is getting worse (Oltsik 2017).

This paper propose a new approach, Cybersecurity for All (CS4A), to resolve the cybersecurity workforce shortage. An overview of the approach is shown in Figure 1. CS4A aims to establish new pathways for nontraditional computer and information sciences and lifelong learners to become cybersecurity professionals through continuing education.

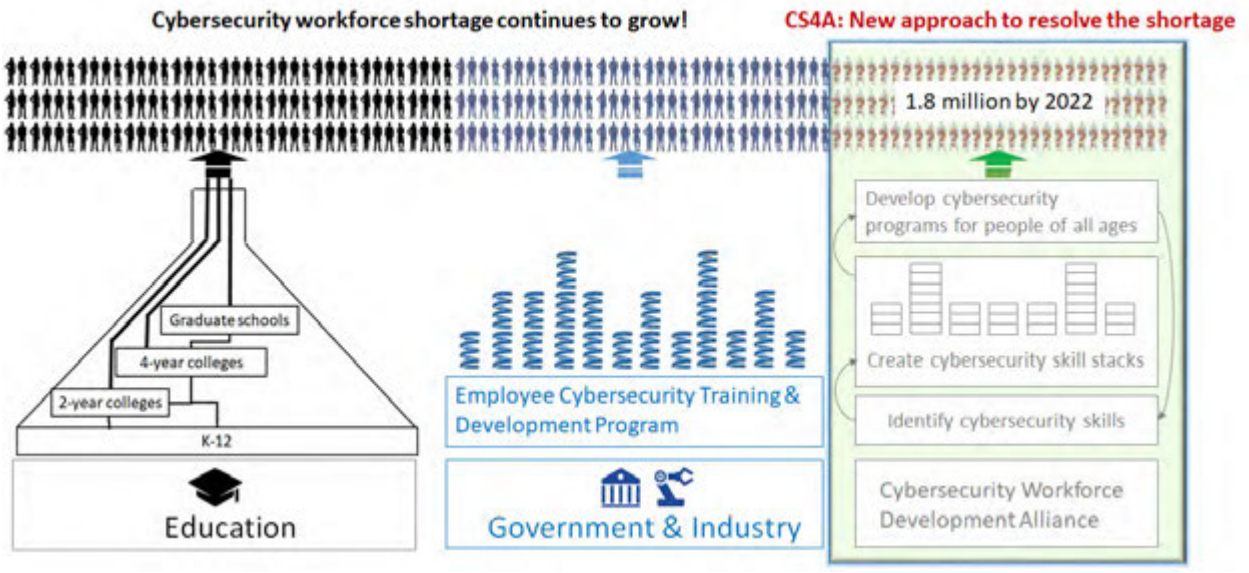


Figure 1. CS4A Overview

II. CS4A: A New Approach for Cybersecurity Workforce Development

A. CS4A Overview

Many initiatives have been put in place to develop cybersecurity workforce. Higher education are adapting curriculums to support cybersecurity program needs. Colleges are taking actions to partner with K-12 and post-secondary schools to engage more students in cybersecurity education. Extra efforts are also being made to attract minority students (e.g., women students) to cybersecurity (A Frost & Sullivan White Paper 2017). In private sectors, many companies and organizations have developed their own on-the-job training programs to train employees to meet their needs in cybersecurity. These endeavors are clearly important and will continue to help build cybersecurity workforce. However, they are far more than enough (Oltsik 2017).

In addition to the traditional academic programs and on-the-job training, the paper proposes a new approach, Cybersecurity for All (CS4A), for cybersecurity workforce development. CS4A targets to a new pool of candidates who are nontraditional computer and information sciences

and lifelong learners. These learners will be most likely declined from any academic cybersecurity programs due to lack of required background. Their daily jobs typically do not involve any cybersecurity duties and will not be able to participate in any on-the-job cybersecurity training. However, they would like to develop their cybersecurity skills through continuing education and prepare them for cybersecurity career in the future. CS4A aims to help this new pool of candidates and help them develop the desired cybersecurity skills. CS4A achieves the goal in three steps: i) identify cybersecurity skills needed to succeed in cybersecurity, create cybersecurity skill stacks to establish pathways to cybersecurity career, and develop flexible and accessible cybersecurity programs for people of all ages.

B. Identify Cybersecurity Skills

The fast changing and sophisticated attacks indicate that the cybersecurity skills needed to prevent those attacks must also be adapted over time. In addition to the skills taught in computer and information sciences, skills such as data analysis and an understanding of risks are also important. To address the cybersecurity skills shortage, it is important to clearly identify what cybersecurity skills are needed to succeed in cybersecurity. This is an important issue for all parties including government, academia, and industry. The paper proposes to form a Cybersecurity Workforce Development Alliance (CSWDA) to lead the efforts. The Alliance includes companies and organizations from both the public and the private sectors.

C. Create Cybersecurity Skill Stacks

Based on the cybersecurity skills identified, the Alliance will create cybersecurity skill stacks which will establish pathways leading to cybersecurity career. Cyberseek (www.cyberseek.org) divides cybersecurity career into three levels: entry-level, mid-level, and advanced-level. The common cybersecurity feeder roles which lead to cybersecurity career includes networking, software development, system engineering, financial and risk analysis, and security intelligence. The cybersecurity skill stacks will establish new pathways for participants to become one of feeder roles as identified by Cyberseek.

The cybersecurity skill stacks will be based on the cybersecurity skills identified in Section II.B. Each stack specifies prerequisite skills required, skills to be developed, and the career path which it may lead to. The cybersecurity skill stacks could be cascaded together horizontally and

vertically. The stacks cascaded horizontally aim to help participants to extend breadth of skills in cybersecurity. The stacks cascaded vertically aim to help participants to develop cybersecurity skills in depth. The stacks will be modulated and can be grouped together based on needs. Certificates can be created for stacks as incentives to participants.

D. Develop Cybersecurity Programs for People of All Ages

Most of the current endeavors of cybersecurity workforce development programs are closed loop. The academic cybersecurity programs are very competitive and selective. Companies and organizations develop training programs to meet their own needs. These programs are generally not available for public. To resolve the cybersecurity workforce shortage challenge, we need to target to a much larger pool of candidates and prepare them to become cybersecurity professionals. CS4A targets a new pool of candidates which are nontraditional computer and information science and lifelong learners. New programs will be developed based on the cybersecurity skill stacks. These programs will be accessible to these learners and also flexible for participants. These new programs may include online programs, vocational schools, certificate programs, etc. The new programs can be sustained with the support from government agencies, academia, and industry.

III. Summary

This paper proposes a new approach, CS4A, to resolve the cybersecurity workforce shortage challenge. Unlike the academic cybersecurity programs and the on-the-job training, CS4A targets to a new pool of talent candidates which are nontraditional computer and information sciences and lifelong learners. CS4A creates new pathways for these leaners to become cybersecurity professionals and thus help resolve the cybersecurity workforce shortage challenge. CS4A can also be used as training programs for students in colleges and continuous training programs for cyber professionals.

References

A Frost & Sullivan White Paper, 2017. *The 2017 Global Information Security Workforce Study : Women in Cybersecurity*, Available at: https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf.

Center for Cyber Safety and Education, 2017. The 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk. *Frost & Sullivan in partnership with Booz Allen Hamilton for ISC2*.

Cisco, 2015. *The Internet of Things : Reduce Security Risks with Automated Policies*, Available at: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/security-risks.pdf.

FTC, 2017. The Equifax Data Breach. Available at: https://www.ftc.gov/equifax-data-breach.

Oltsik, J., 2017. The Life and Times of Cybersecurity Professionals: A Cooperative Research Project by ESG and ISSA. , (November), p.9. Available at: http://www.esg-global.com/.

Suby, M. & Dickson, F., 2015. *The 2015 (ISC)2 Global Information Security Workforce Study*, Available at: http://www.csoonline.com/article/2922381/infosec-careers/confronting-the-widening-infosec-skills-gap.html.

The White House, 2017. President Trump Protects America's Cyber Infrastructure.

Dr. Yong Wang is an Associate Professor in the Beacom College of Computer and Cyber Sciences at Dakota State University. He received his B.S. and M.S.E degrees in Computer Science from Wuhan University (China) in 1995 and 1998, respectively. He received his Ph.D. degree in Computer Science from University of Nebraska-Lincoln in 2007. Before he joined DSU in 2012, he had spent 10 years in telecommunication industry as a senior software engineer and a team leader. His research focuses on network security and privacy issues. His current research projects include mobile, cloud, IoT, and big data. He has published 50+ peer-reviewed papers in prestigious journals/conferences. He is a co-author of three books. He also severs as Technical Program Committee (TPC) members and reviewers for many international conferences in Computer Science. Dr. Wang received four awards from National Science Foundation between 2012 and 2017. He is currently leading the NSF CyberTraining project at DSU.

Ideas (1188 words)

This paper considers the following questions (from **https://www.cerias.purdue.edu/site/nace/**):

- What are the most acute cybersecurity labor supply issues the United States will face in the next 5, 10, 15 and 20 years?
- To address these labor supply issues, what new approaches to cybersecurity education are most needed and why?
- How do we get more US citizens—and a more diverse population —into cybersecurity in meaningful ways?
- What are the proper levels of education to address?

As systems and networks in nearly every industry are increasingly leveraging the efficiencies of the internet, from premise-based to cloud solutions, the relevancy of cybersecurity within these industries increases in like manner. Cybersecurity is integrated throughout each sector of modern society – retail, finance, health, cities, suburbs, schools, workplaces. The pervasiveness of cybersecurity places a heavy demand for individuals who can identify, protect, detect, respond, and recover. If significant changes are not made in how cybersecurity education is approached, the most acute labor supply issues, whether 5, 10, 15, or 20 years out, will be in:

1. Security Engineering – designing security into the vast amount of "things" that will connect to the Internet, especially things that have physical and life/death ramifications if compromised; and
2. Diversity within Machine Learning and Artificial Intelligence – the data used to train machines, and the personnel involved in creating the algorithms for machines and AI, must be accurate, and representative of the population served by the machines, respectively. Otherwise, we will have the same bias in "robots" as we have in human beings, except without the potential counterbalancing aspect of human compassion, or change of heart.

The labor supply issue is an issue of numbers, specifically the number of available, appropriately trained, experienced, and trusted professionals. There are ample United States citizens to address the U.S. cybersecurity shortage, but underrepresented populations must be engaged, starting at

early ages, to address these gaps. There are several barriers that inhibit currently underrepresented populations from becoming successful cybersecurity professionals. Primary inhibitors include:

1. Lack of awareness (e.g. no role models who look like the students, or otherwise, within their everyday environments, and few role models who look like them in mainstream media who, even fictitiously, are in the cybersecurity field);
2. Lack of access (e.g. no computers at home, antiquated or non-existent computers at school, limited transportation to camps or other facilities);
3. Lack of basic needs (refer to Maslow's hierarchy of needs) such that self-actualization in a specific career such as cybersecurity, is fleeting, and quite difficult to obtain;
4. Lack of academic support (e.g. overcrowded classrooms, single parent homes or parents with multiple jobs and limited education that can help with understanding cybersecurity); and
5. Institutionalized discrimination (e.g. the current elementary to prison pipeline, disproportionately, and adversely, impacts minority students).

Exposure to cybersecurity related careers must happen as early as elementary school to plant the seeds of possibility for students. Exposure to these careers must come in the form of classroom learning, after school enrichment, and mentorship, with proportionate representation from role models who look like the students. The students must be able to see themselves – black boys seeing black men, Hispanic girls seeing Hispanic women – in their instructors, in their tutors, and in their mentors. Employers with strong diversity programs can partner with schools, and include mentorship of students as a formal part of employee career development and performance evaluation. Mentorship can be done in person, or accomplished via an online means to expand the reach of each mentor, and better scale the number of students the mentor can effectively impact.

Schools with stretched resources and budgets can also partner with companies to establish a technology endowment program so that technology, while still largely current, can shift from a company to a partnering school. In this way, students have access to learn in a hands-on way, using relevant technology.

The lack of basic needs and academic support are not easy problems to solve, and certainly require the participation of family, community organizations, government, and industry. The approaches taken to meet basic needs and provide ample academic support must be sustainable, and based in an economic model that educates and empowers, not only the students, but their family and social network.

Cybersecurity is a field that requires trusted individuals, and students must learn early on that antisocial and criminal activities can drastically impair their ability to participate in such promising fields as cybersecurity. This is another reason why exposure to cybersecurity education and careers should start as early as elementary school, so that children can start making decisions consistent with a field they may find interesting.

Publicly traded privatized prison companies use student test scores, starting from as early as third grade, and other student home factors to project future prison populations. Schools are using policing in a way that criminalizes student behavior without addressing root causes. If algorithms and school policies can be created and used to project and yield a negative outcome and situation for students, then the same algorithms and policies can be turned on their head and used as a means to identify populations to target for technical skills training and education that lead to lawful, promising careers in fields such as cybersecurity. The pipeline to prison must be disrupted to redirect the talent to a cybersecurity pipeline instead. Some of our country's most brilliant minds are put behind bars at early ages, and perpetually trapped in the justice system, but these brilliant minds can be tapped to address instead a dire need in our country.

Cybersecurity education should be approached in a way that demonstrates how cybersecurity is present in the everyday lives and interactions of students. In this way, learners are able to make a connection between the broad term of "cybersecurity" and their everyday lives. Further, to make cybersecurity more accessible to broader populations, cybersecurity education should be approached by making analogies to long standing and understood systems, environments, and principles. As an example, computer networks can be compared to a home; intrusion detection systems can be compared to home alarm systems; computer viruses can be understood through comparison to human viruses. While cyberspace is a "new" domain, there are multiple long existing domains that can be used as a basis of comparison and learning for cybersecurity. This approach to education is already happening with such disciplines as biomimicry, where biological systems are used to drive the design and function of computer networks.

This "teach by analogy" approach to education would include the following broad steps:

1. Identify the industries, systems, and other aspects of the target learner population's everyday environment (e.g. inner city, reservation, rural);
2. Leverage the target learner population's understanding of their everyday environment to explain cybersecurity concepts;
3. Engage learners in opportunities to think through solutions that apply to their everyday environment, and then challenge them to extend the solutions to convey the analogous application in cyberspace;
4. Provide access to the tools necessary for the learners to prototype and demonstrate their cybersecurity solutions.

By approaching education in this way, learners are trained to see cybersecurity as an integrated, multidisciplinary field with broad applications in everyday life.

Author Biography (158 words)

Tina C. Williams-Koroma – Esq., CISSP, PMP, is founder and President of TCecure LLC, a cybersecurity services company based in Maryland. Tina has 15+ years of experience working in the cybersecurity field, providing services to public sector and commercial clients. She possesses a B.S. in Computer Science from the University of Maryland Baltimore County (UMBC), a M.S. in Management from Rensselaer, and a J.D. from the University of Maryland Francis King Carey School of Law. She is a member of the Maryland Bar and the CyberMaryland, NICE365 Industry Advisory, and UMBC Research Park Boards of Directors, and is an Adjunct Instructor at UMBC for the Masters of Professional Studies in Cybersecurity. Further, through a TCecure contract with the University System of Maryland, Tina is the Cybersecurity Academic Innovation Officer for the National Cybersecurity Federally Funded Research and Development Center (FFRDC), responsible for integrating academic research and resources into the National Cybersecurity Center of Excellence (NCCoE).

CybSec Champions Fellowship

Purpose/need: There has been great attention on the need to fill the cyber security work force. With the focus largely on college students and veterans re-entry into the work force, recently, the focus has been shifted to high school age and under. Providing programs targeted to this age group has started with competitions such as CyberPatriot and CTFs and programs to support specific groups such as girls through avenues like Aspirations in Computing and Girls Who Code, people are understanding the need to start training and supporting the younger generation. Without planting the seed at a younger age, there will continue to be a shortage in supply for the cyber security workforce. Without having young people grow up with the vocabulary of security in this technology driven world, there will never be a shift in culture that embraces security as an integral part of ensuring the balance of the cost of technology.

I propose the missing piece in the work that is being done in the investment in the people investing in the development of these young people. "Champions" that have been fighting to ensure that young people are being exposed to opportunities will not only better the young person's future, but will also contribute to the betterment of the world. Champions might be school teachers or girl scout leaders or after school providers, but they all share similar traits: be passionate about their vision of what the world should be like and be willing to put in the work to see it happen (evidenced by the countless "volunteer" hours of work they dedicate), be passionate about the hope they place in young people, have an understanding about the system we live in (economic mobility only exists if young people are trained in an area that they will have an opportunity to find work), and look at the world in the broader sense (in order for us to be "safe," we must be the ones defending). Like super heroes, these champions view their role in society as agents of change with a code that they live their lives by. This population of people can often be found coaching cyber competition teams, starting a chapter of a local Girls Who Code group or volunteering to be a Girl Scout leader. There are few resources widely available for these champions to develop and be even more supportive to the young people they work with. However, champions have learned to be resourceful and forage along the way and find what they need along the way to be the best champion they can be for the young people they work with. There needs to be a system (program) in place to support the people supporting the young people so that this pool of talent can even make it to the next level, which could be college or directly to the work force.

Roles/players:

Champion: Teacher, Community volunteer, after school provider or anyone else not in a traditional role that is supported but would benefit from professional development/mentoring specific to the cyber security field.

Mentor: A person at an institution of higher learning or even an industry partner dedicated to being part of the pipeline of ensuring the growth of the pool of applicants in the security field. Willing to invest time and resources to be a part of a team of adults supporting the young people the Champions work with.

Program Manager: Someone who is overseeing the implementation of the program and ensuring documentation and paperwork is being handled accordingly.

Program overview: Cohort of Champions will be chosen and matched with Mentors in their state. Reason, so that they are able to create a local support network. On average, about 72 percent of high school students stay in state when attending college (www.statisticbrain.com/percentage-of-out-of state-students-at-public-universities). This will give the Mentor who works an edge in encouraging these students to attend the school he/she represents. He/she will have developed a relationship and support the young person in his/her transition, a continuation of support through the "pipeline." For an Industry Mentor, his/her role can be and not limited to helping plant the seed of the end goal, of finding work and supporting the steps necessary to get there. Benefit for Industry partners (mentors) is a pool of young people they would be able to recruit to work for the Industry partner's company, either right out of high school or out of college. The perfect triad would be Industry, Higher Ed, and the Champion. Benefits for the Higher Ed Mentor would be to link his/her students with Industry partner as well. Champions would benefit from the resources provided by his/her mentors to bring back to students. From curriculum to pool of people to bring in for career awareness opportunities, everyone would benefit.

Program Components:

- Champion would meet with Mentor(s) at least once a month to check in on needs and opportunities. This could be done virtually or in person. Ideal situation would be to meet, then to also meet with students participating.
- Champion would have an opportunity (funding) to attend at least 1 conference for development and networking opportunities.
- Champion will work with Mentor(s) to develop a project/research to further the development of cyber education. Examples, but not limited to gamifying cyber security, curriculum for high school or middle school aged students, events to target growing interest in cyber security, especially in underserved areas. Project/research would be presented at an event such as CISSE and/or locally at an ISSA event.
- Champion and possibly Mentors will receive a stipend for their commitment to the Fellowship.
- Champion will commit to minimum of 1 year. Possible to grow Fellowship to 2 years if he/she returns as a Mentor to next cohort.

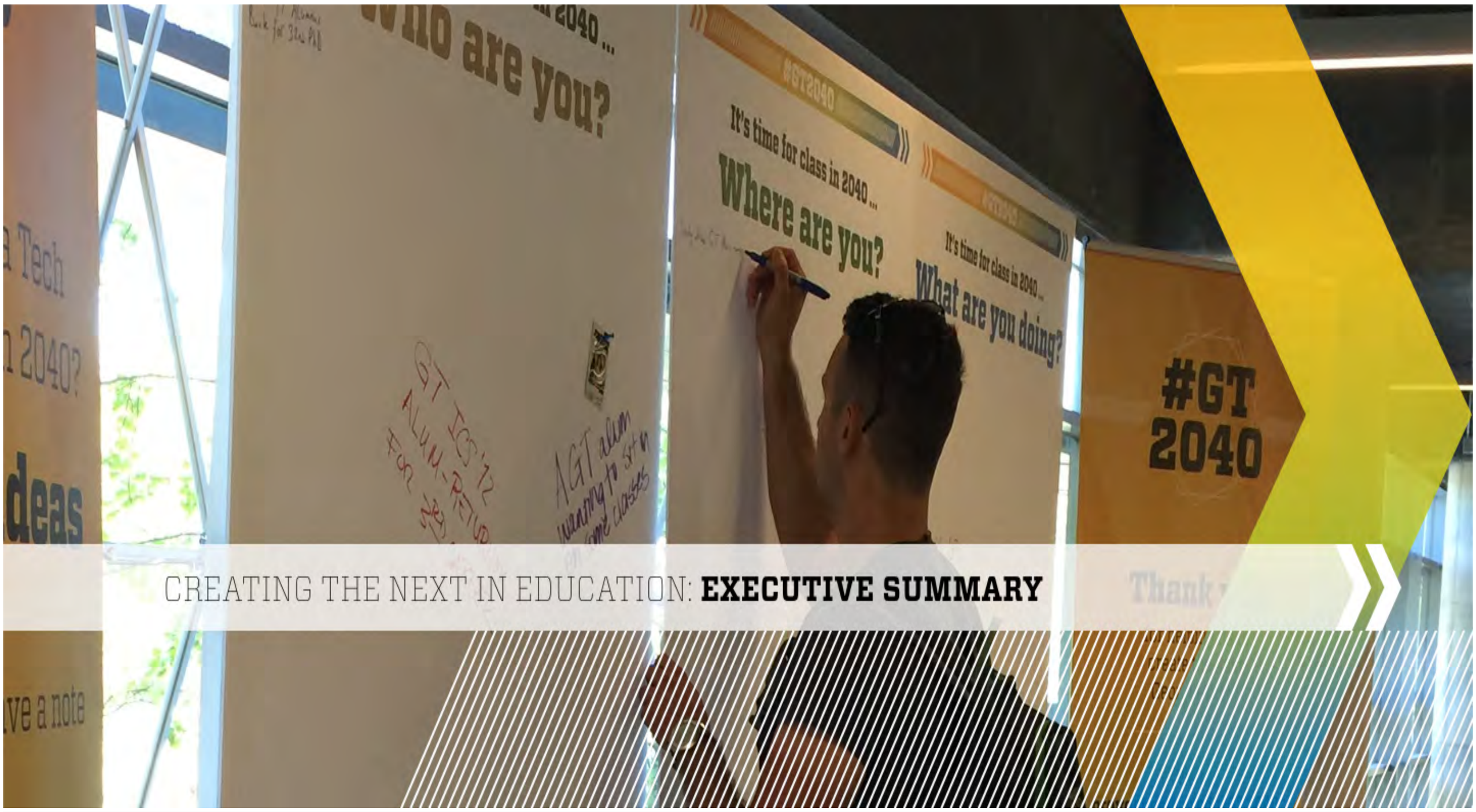
Qualifications of Champions/Who should apply?

- Majority percentage of applicants should be people with a proven track record of their commitment to cyber security education to middle and high school students.
- Small percentage of Fellows should/can be newbies who are looking for help getting started.
- Works directly with middle or high school youth (preference given to those working with underserved communities)
- Benefit from a mentorship to grow the work that they are currently doing

Outcomes:

- Project or research that is developed by Champion (deliverable).
- Still not sure how to measure student success—possibly the number of students served by the Champion that go into Cyber Security as a major/minor or go into Industry out of high school.
- TBD

There are still a lot of questions and details to work out, but I believe this is a strong start to the discussion of the need to include and support the role of the Champion who sometimes do not fall into traditional titles and therefore is not supported to continue the work that they do. Access, opportunity and support are the key factors that I feel are lacking for Champions currently. Many Champions have managed to navigate and find a way despite the lack of real direction and support, but I propose that there is a way to provide that support. I believe a program such as the CybSec Champion Fellowship could be valuable as one approach to address the need to educate and help the direction of cyber security.



Executive Summary

This moment is ripe for change in higher education. Scores of technology entrepreneurs, foundations, and policymakers are already trying to shape what the future looks like for both learners and institutions. The message for colleges and universities is clear: they can either sit idly by or join in to design their own destiny. As a selective public institution with a history of educational innovation, the Georgia Institute of Technology sits squarely in the middle of the forces shaping higher education. It is uniquely positioned to model what the university of the future might look like.

This report of the **Georgia Tech Commission on Creating the Next in Education (CNE)** is an effort to draw with broad strokes the nature of education that defines the technological research university of the year 2040 and beyond. The Commission was formed because many within the institution are convinced that by the second half of this century Georgia Tech will be different from the university that matured and prospered in the nineteenth and twentieth centuries. Georgia Tech's mission seems to demand that the Institute examine the choices that lie ahead and make plans for a future that, however uncertain, is bound to present opportunities and challenges that cannot be understood as incremental changes in the status quo.

Drivers of Change

In a prior report titled *Discovering the Drivers of Change in Higher Education* (Georgia Tech 2016), the Commission outlined the forces likely to affect Georgia Tech, including a new and accelerating revolution characterized by technology-driven disruptive change throughout society, shifting public attitudes about the role of public universities, and demographic trends that challenge long-held assumptions about who will benefit from a college education. Upon publication of that report, the Commission engaged in a broad search for ideas about how best to anticipate the kinds of changes that are certainly in store for Georgia Tech and to synthesize a roadmap for the future.

The Georgia Tech Commitment

The overarching recommendation of the Commission is an ambitious proposal called the **Georgia Tech Commitment to a Lifetime Education**. It is a concept unlike anything that exists today—a future for college not conceived solely just as a physical place one enters at a particular age and exits when a degree is completed but rather as a platform for an increasingly diverse population of learners.

By the year 2040, Georgia Tech learners will be more ethnically and socioeconomically diverse. Some will be much younger than traditional undergraduates; others will be much older. Neither group will resemble the traditional, residential college student in terms of their expectations or demands. Their numbers may far exceed the current residential enrollment. The Georgia Tech Commitment is a promise to these new learners to provide the rigorous, high-quality experience that has defined a Georgia Tech education for more than 130 years but to do it in a way that is individually personalized and sustainable for a lifetime. This commitment is a promise to invest in the success of all Georgia Tech students.

For the Georgia Tech Commitment to become a reality, the Institute must redefine its fundamental approach to educational delivery with four key actions: eliminate artificial barriers between college and pre-college schooling, invent flexible educational pathways and credentials that recognize continual learning, reinvent the physical presence of a university for a worldwide population of learners, and provide advising and coaching networks that serve the lifetime needs of Georgia Tech learners of all ages.

Innovation is required for each of these steps to be successful. An integral part of delivering on the promise of the Georgia Tech Commitment is a set of initiatives that are aimed at closing knowledge gaps, prototyping new products and services, and building technological infrastructure that enables this broad expansion of Georgia Tech's mission.

These initiatives are conceived as research programs that will be launched upon completion of the Commission's work. They will be planned and managed by an expanded ecosystem for educational innovation.

The Initiatives

The Commission identified five initiatives to better understand the challenges standing in the way of achieving the vision of the Georgia Tech Commitment and to create tools, invent methods, and collect data that will be required to make progress. Included in these initiatives are immediate actions and longer-term projects that will require both invention and sustained research. These initiatives address problems that the Commission believes are on every critical path to the Georgia Tech Commitment and many other conceivable futures as well.

Initiative 1: Whole-Person Education

Georgia Tech graduates have a reputation for strong technical skills and initiative, but, increasingly, other skills are needed for success in the twenty-first century workplace, including cognitive skills, such as problem solving and creativity; interpersonal skills, such as communications and leadership; and intrapersonal skills, such as adaptability and discipline. The Commission found that virtually all employers consider these skills to be a distinguishing characteristic for long-term success. Employers look to leading colleges and universities to provide graduates who have not only deep disciplinary knowledge but also these additional skills.

This initiative consists of four interrelated projects that address important aspects of delivering whole-person education to Georgia Tech learners:

1. Experiential learning that embeds the learning experience in authentic, relevant contexts.
2. Globalization at home to develop a culture in which critical thinking and collaboration can be taught in the context of a multicultural world.
3. Professional development of graduate students that fuses whole-person education with the more research-oriented training typical of graduate education.
4. A new whole-person curriculum that emphasizes interpersonal and intrapersonal dimensions of education in addition to cognitive dimensions.

Initiative 2: New Products and Services

To meet the demands of evolving job markets and the desires of a widely disparate population of future learners, the Georgia Tech Commitment calls for flexible learning experiences and continual learning opportunities. New products will need to be created that afford future learners the ability to customize their educational experiences. Development of these new educational products and services will be enabled by four projects that address both near-term and long-term problems:

1. Microcredentials to create more efficient packages of experience and achievement.
2. A matrix of minimester classes that will allow students to replace monolithic three-credit-hour classes with more granular and flexible modules.
3. A new credit-for- accomplishment unit measured by demonstrated competencies and skills.
4. A new decentralized transcript based on blockchain technology that allows students to combine evidence of learning and achievements into credentials that are relevant to potential employers.

Initiative 3: Advising for a New Era

Advising for a new era is a challenge to the traditional fragmented approaches to advising. The Commission recommends a robust learner data backbone as well as artificial intelligence assistants that integrate prescriptive, intrusive, and developmental advising services to personalize them and provide a new advising experience, at scale, to learners of all types. Three projects are key to launching this initiative:

1. Personalized advising for effective and scalable advising services tailored to the needs and prospects of individuals at all stages of life.
2. Technology-enhanced advising to deliver new ways for supporting personalization at scale.
3. Personal Boards of Directors to create professional networks for Georgia Tech learners.

Initiative 4: Artificial Intelligence (AI) and Personalization

Georgia Tech has led in the development of AI-based personalization systems. The "Jill Watson" experiment used the IBM Watson system as the basis for an artificially intelligent teaching assistant and was widely hailed as a breakthrough in both AI and educational technology. The opportunity now exists to augment "Jill's" skills to handle other tasks that are associated with personalized learning. A multifunction virtual tutor can be deployed to advisors, coaches, and even mentors located at distributed Georgia Tech locations around the world. Three projects are envisioned as part of this initiative:

1. Pilots for mastery-learning and adaptive-learning platforms that can put the kind of technology that will allow customized delivery of material into the hands of learners within two years.
2. Personalized and multifunctional tutors to take advantage of advances in AI to push the envelope in personalized learning.
3. Human-centered AI to support the development of interactive AI agents whose interactions with humans are informed by cognitive models and contexts.

Initiative 5: A Distributed Worldwide Presence

The idea of a physical campus—a designed space for students, teachers, and educational programs—has been a mainstay of the college learning experience for a thousand years. The physical campus is, however, a fragile model. A campus has the advantage of making educational facilities broadly available, but it does not necessarily match services to regional needs.

The Georgia Tech Commitment values the personal presence of instructors and advisors in the educational experience but recognizes that problems of scale and expense will limit the number and kind of such deployments. It is always an option to provide remote or online facilities to connect new students to a central campus, but Georgia Tech's experience with affordable online master's degrees convinced the Commission that there are better ways to create a real presence as part of the Georgia Tech learning experience. The following projects will enable experimentation with new modes of student interaction:

1. *The Georgia Tech atrium*™, a concept that recreates in other locations the scalable gathering places and portals to educational services that have become ubiquitous on Georgia Tech's central campus. These spaces can be located near clusters of Georgia Tech learners in co-working spaces, corporate offices, or even retail malls. Each atrium can be programmed to suit the needs of local learners and can provide cost-effective, high-quality educational experiences to Georgia Tech students and others by matching personnel, expertise, and facilities to the needs of the communities served.
2. *A Living Library for Learning (L3)* that expands an already successful network of Human Libraries to a broad range of educational contexts. Through an L3 portal, Georgia Tech will be able to provide personal, on-demand access to individuals who have first-hand experiences to relate to classes or individual learners. The Human Library vision of "loaning people, not books" has great appeal for technological universities.

The Culture of a Deliberately Innovative Organization

The five initiatives represent radical departures from usual ways of delivering rigorous university-level learning experiences. The pace of innovation required to achieve their goals is daunting. Recognizing the often-slow pace of change in higher education, the Commission envisions a long-term process for instilling in the culture of Georgia Tech the ability to innovate in a more predictable and timely way, moving to becoming a more deliberately innovative university.

The Georgia Tech Lifetime Commitment and the initiatives proposed to achieve it are bold, and they need to be supported by an underlying culture of educational innovation that is both robust and agile so that it can adapt to disruptive forces and a rapidly increasing rate of change in technology and society. Georgia Tech's current culture has produced internationally recognized innovations in education that have had great impact, but the Commission feels there are still cultural shifts that would improve the university's capacity for continuing innovations. By making innovation processes the subject of study and applying research-based methodologies, the Commission believes that Georgia Tech can become a more deliberately innovative organization.

A systems approach would allow the examination of innovation processes in interacting groups of people and organizations, and it would support taking deliberate actions to improve desired outcomes over time. The Commission envisions five steps that are necessary to launch the Institute onto this pathway.

Merging Two Successful Cultures

Georgia Tech's capacity for educational innovation has grown dramatically over the past decade, but to a large extent, successful innovation in education is still not systematic. Inventions germinate and successfully change the way education is delivered, but success or failure seems to depend as much on luck or circumstance as on merit or need. The Commission imagines a merger of two existing, successful cultures for innovation: a grassroots culture and an institutional culture. Each culture is individually effective, but aligning the two will create a more agile and sustainable environment for innovation.

A Systems Approach to Becoming Deliberately Innovative

A systems approach to creating a deliberately innovative organization improves on current successful models of innovation. The Commission recommends long-term steps to immerse educational innovation practices in the kinds of cultures that are known to enhance innovation at the enterprise and organizational levels, shifting academic structure and processes when necessary to better align with those known to promote innovation.

Enhancing the Innovation Ecosystem

The Commission examined ways that the current educational innovation ecosystem might evolve into a broader, more coordinated entity, with expanded scope and range. A great advantage enjoyed by Georgia Tech is its vibrant research environment. The Commission recommends fusing the values and mindsets of research and education communities at all levels of university operation and governance.

Bridging Organizational Silos

Organizational silos are policies, procedures, or cultural limits that inhibit people of different groups from free interaction. An academic example is disciplinary silos. New organizational and financial models will help to bridge these silos.

Motivating Individuals in the Innovation Process

The Commission recommends policies that acknowledge, reward, and incentivize faculty and department leaders to pursue educational innovation. Everyone at Georgia Tech should be immersed in a culture of educational innovation. Every investment decision should be steeped in it. The Commission endorses total immersion, but it will take time to create conditions that connect the individual goals and aspirations of Georgia Tech's faculty and students with the goals of the Georgia Tech Commitment. It is an opportunity for individuals to grow by leveraging what they know while being honest about what they do not know and by taking risks while thinking through worst-case scenarios.

What's Next?

Demographic and economic forecasts gathered during the six-month discovery phase that kicked off the Commission's work paint a clear picture: higher education institutions of all kinds are facing a far different future compared to the world to which they have become accustomed. In many ways, the current challenges facing

higher education are similar to the ones that confronted Georgia Tech at its founding. Today's challenges, like those of the mid-nineteenth century, are the consequence of rapidly expanding knowledge, industrial revolution, and immense change in the world economy.

In the previous era, colleges and universities and their leaders approached those changes with great optimism and a feeling that change was an opportunity for growth. The Commission believes that spirit can be rekindled today. A group of universities will need to lead higher education through the changes promised in this next decade and beyond. Georgia Tech is determined to be in this group by expanding its mission to include the Georgia Tech Commitment to a Lifetime Education.

The roadmap presented here is a result of looking up and out to grasp the bigger picture of higher education and its future. We imagine a future where artificial barriers that have existed in education disappear and the role that people and technology play in guiding students in their lifelong educational journeys is better understood. In such a future, new educational products will be needed, and, as simple skill acquisition becomes easier to achieve, the whole-person education needed to prepare individuals for new workplaces will become an essential part of higher education. Finally, the success of all the projects described in this report is predicated on an immersive culture that fosters deliberate innovation.

Access to higher education and scholarly research has long been the lever universities have pulled to promote their prestige. In higher education it is difficult, if not impossible, to stray far from the pack and think differently about how to engage new generations of students and how to provide them with the most immersive educational environment, all while being on the cutting edge of the next discoveries in the world. But the changing needs of both the global economy and higher education demand that universities like Georgia Tech move in a new direction to remain relevant in an increasingly automated and diverse world.

Timeline of Commission Activities

View Full Size

« Previous Page: Report Home

Next Page: Introduction »