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).