A Holistic Approach to K12 Cybersecurity Education

Giti Javidi¹, Ehsan Sheybani², Zacharias Pieri³

¹Information Technology, University of South Florida, Sarasota, Florida, USA
²Information Systems and Decision Science, University of South Florida, Sarasota, Florida, USA
³Social Sciences, University of South Florida, Sarasota, Florida, USA

Abstract - In this paper the authors describe their innovative methodology to expose high-school teachers to deeper learning for engagement that seeks to connect wireless and internet technology leadership through inspiring inner creativity and critical thinking in cybersecurity. This is to address the need for qualified technology teachers, student access to wireless and web-based cybersecurity experiences, and the role of leadership in technology in response to the evolving digital ecosystem. The idea is to train the teachers to serve as advisors to students by developing strategies for fun-learning activities (e.g., Hackathon, Shark Tank, and Maker-Space) and integrating cybersecurity technology in the curriculum. Using wireless and internet technologies, they learn strategies to encourage students to solve social problems with creative business-based solutions. As a result, students will enhance tech skills, discover new career directions, and build their online brand. Their network will be enriched by partnerships with industry and tech leaders. The goals are to expose K12 students to technology career fields in cybersecurity, establish tech innovator model for entrepreneurial thinking, deliver an online resource to disseminate curriculum, and promote an enriched ecosystem model for cybersecurity learning in K12.

Keywords: K12, Curriculum, Cybersecurity, Modular, STEM

1 Introduction

The web-based and wireless cybersecurity skills shortage is reaching prevalent proportions. The consensus in the STEM community is that the problem begins at K12 schools with too few students studying STEM subjects. In the field of cybersecurity, this issue becomes more trivial since organizations can’t afford to underestimate their exposure to cyber-attacks and the importance of cybersecurity. Increasing cybersecurity professionals is a necessary solution to the cybersecurity skills crisis in the technology industry. One way to ensure a larger pipeline in cybersecurity is to train more K12 teachers to not only teach cybersecurity in their schools and/or integrate cybersecurity concepts in their classrooms but also to promote IT security as an attractive career path. The gateway to our next, best generation of tech-savvy workforce is training high-quality teachers since they are the most influential element in shaping and guiding a student's educational path.

To prosper in the world of rapidly changing technology and the required technological skills, the proposed curriculum will also incorporate leadership knowledge and soft skills as necessary elements for any STEM worker. Our approach is to develop a curriculum that will combine all those necessary skills to provide a meaningful opportunity to engage students with the real-world cybersecurity issues that industry grapples with. This curriculum will initiate an effort in the cyber-technology education in K12 and cultivate leadership talents with creative thinking, and practical ability. By introducing important elements of change in K12, there is an opportunity for innovation in computing, which drives economic growth and underlies many scientific advances.

The huge shortage of personnel with sufficient knowledge, skills and abilities in cybersecurity field is already taking a toll locally and globally. Part of this deficiency is due to absence of minorities and women in technical fields (population issue). The other contributor to this problem is the lack of encouragement, interest, and engagement at the K12 for students to find careers in challenging fields such as cybersecurity (pipeline issue). To remedy this, the authors have taken an innovative approach to design and develop a modular K12 cybersecurity curriculum. The innovative techniques and modules used in the proposed curriculum to incorporate cybersecurity concepts include, but are not limited to:

1. Taking a holistic approach to make cybersecurity awareness the minimum requirement for K12 college-bound students,
2. Using a train-the-trainer model to train K12 teachers to teach cybersecurity, integrate cybersecurity concepts in their classrooms, and promote cybersecurity as an attractive career path,
3. Introducing creative, modular, and hands-on activities to teach programming, networking, and other cybersecurity-related topics in a fun and attractive manner,
4. Developing case studies, real-world examples, and projects that connect cybersecurity concepts to terrorism and radicalization, social, political, and financial hacking, military strategic missions, recruitment of extremist and religious groups, etc.,
5. Adding leadership and entrepreneurship skills to the mix to prepare students for real-world problems.
6. Assessing the delivery methods, timing, format, pacing, and outcomes alignment to provide a baseline for future research.

2 Research and Methodology

Design and development of a modular, scalable, and novel cybersecurity curriculum will help train the future workforce. This will be done in coordination, integration, and collaboration with other/existing programs to leverage and/or expand STEM educational research. The design and development of modules in the proposed curriculum was done considering the following aspects:

2.1 Taking a holistic approach to make cybersecurity awareness the minimum requirement for K12 college-bound students

Although considerable growth in computing jobs is expected in the next decade, students are not majoring in computing in sufficient numbers to meet this demand. Cybersecurity is one of the most serious economic and national security threats facing our nation today. According to the Bureau of Labor and Statistics, the rate of growth for jobs in cybersecurity is projected at 37% from 2012-2022, higher than the average for all other occupations [1]. Hence, the demand for cybersecurity professionals is soaring. Addressing the achievement gap by leveraging an emerging group of K12 students is a key strategy to consider.

2.2 Using a train-the-trainer model to train K12 teachers to teach cybersecurity, integrate cybersecurity concepts in their classrooms, and promote cybersecurity as an attractive career path

The proposed curriculum creates a partnership with local K12 teachers to help them build knowledge, skills and confidence in cybersecurity, who in turn, can help engage students in STEM learning and prepare them for success in STEM careers. By helping more teachers become proficient in teaching cybersecurity, at an earlier stage, more young people will become aware of the career opportunities and prepare themselves for technology-related education at the university level, which, ultimately, will help tackle the technology workforce deficit in the United States. Maintaining a “STEM-interested” student body can potentially have significant long-term implications. In today's competitive work environment, the required technical skills are not enough for future employers. This curriculum will equip students with the requisite combination of technical and soft leadership skills needed to excel in the field of cybersecurity. For example, teamwork is a critical skill in cybersecurity as organizations often are made up of tens or even hundreds of information technology/security members. Collaboration is required for incident handling, digital investigation, implementing technical controls, enforcing policies, and so many other responsibilities required of a cybersecurity professional. The curriculum also follows the basic principles of leadership education including pushing for a deeper understanding of learning, encouraging students to challenge the status quo, thinking outside the box, understanding the marketing behind a solution, building strong relationships through networking and collaborating with others. Better innovation, development and research on leadership education improve the spirit of students and are essential to reducing the number of educated unemployment [2, 3, 4, 5, 6, 7].

2.3 Introducing creative, modular, and hands-on activities to teach programming, networking, and other cybersecurity-related topics in a fun and attractive manner

Robotics, video games, music, and movies are some of the fun and attractive ways in which creative, modular, and hands-on activities in programming, networking, and other cybersecurity-related topics can be taught. Computers have become indispensable in robotics, video game, music, and movie making, distribution, performance, and consumption. Students need to learn how to use computing to explore powerful and creative ideas. Introductory computer science courses at each level of K12 is needed to give students a broad perspective of computing and its impact. These courses should also be designed in a way to attract diverse populations including females and underrepresented minorities.

2.4 Developing case studies, real-world examples, and projects that connect cybersecurity concepts to terrorism and radicalization, social, political, and financial hacking, military strategic missions, recruitment of extremist and religious groups, etc.

For a curriculum to be current and applicable, it would have to have case studies and real-world examples. Today's technology world has many cases that can be presented as valid projects for a cybersecurity curriculum. While the rise of social media sites such as Facebook, Twitter, and YouTube have been heralded as innovative platforms that serve to connect individuals, communities, and ideas across the globe, they have also been exploited by violent extremists to radicalize and recruit individuals to their causes [8]. A prime example of this has been Islamic State’s ability to master social media in effective ways to reach vulnerable populations, and despite social media operators’ efforts to block terrorists from influencing their networks, each new terror attack spawned more chatter, imagery, and propaganda [9]. Social media
allowed Islamic State to amplify their message, giving them access to spaces and audiences without consideration for physical borders. Indeed, recruits to the Islamic State based in Syria and Iraq included people from over 100 countries, and their relative youth was a further signal that the use of social media was important in their radicalization and recruitment [10]. Content has included propaganda videos exalting the virtues of the given group’s narrative, but it also afforded more personalized interaction between extremists and those being targeting through message boards, and the creation of specialized online training sites [11]. Removing such content is a challenge, since Facebook has around 1.6 billion user accounts, YouTube around 1 billion active accounts, and Twitter with 336 million regular monthly users.

One aspect that governments and security agencies are investing in is that of countering violent extremism online, and social media companies are being urged to develop and implement automated technologies to identify extremist content that can then be combated. This is something that is already being implemented with some degree of success, for example many ISIS affiliated accounts on Twitter have already been closed down [12]. Automatically being able to identify and delete extremist content from sites is one method of dealing with the situation, though, perhaps, a more effective one is that of “taking on” that content and developing resonant arguments to challenge it. With regards to Islamic State, Islamic scholars can be engaged to develop counter arguments with solid Qur’anic justifications that can then be presented as counter-arguments in online forums and social media sites [13].

### 2.5 Adding leadership skills to the mix to prepare students for real-world problems

While K12 students go through various courses that teach them proper typing, basic search engine usage and computer program training, they are not being taught about the soft skills associated with these technologies. While much has been reported on increasing participation in computer science and other STEM fields, little has been reported on the specifics of leadership in cybersecurity. There are also significant misconceptions about careers in cybersecurity and the backgrounds of value to this field [14]. The proposed curriculum will also provide technical as well as non-technical knowledge and skills necessary for cybersecurity, awareness about cybersecurity issues and tools for prevention and various resources to build foundational knowledge and skills for a career in cybersecurity. Educators are provided with various curriculum resources and programs to help identify the skills and knowledge students need to become members of the growing cybersecurity community.

### 2.6 Assessing the delivery methods, timing, format, pacing and outcomes alignment to provide a baseline for future research

The proposed curriculum has a built-in assessment instrument. The mixed-method evaluation has two main goals: (1) formative evaluation of curriculum planning and implementation; and (2) summative evaluation of learning outcomes for participants. Although the main interest would be in comparing pre-to post-test scores, interim assessments will permit the evaluators to assess whether there are differences between continuing participants and those who drop out. The constructs measured by the assessment survey, with items borrowed from pre-existing, validated instruments whenever possible includes the following: demographics; attitudes toward computer and technology tools; participation in IT-related showcases; knowledge of STEM careers; interest in and understanding of app design; and understanding of educational and social effects in programming and app generation.

### 3 Results and Discussion

Through focused activities, adopted into an environment where a dearth of Tech-Ed (or STEM Ed) currently exists, there is genuine potential for dramatic results. The proposed curriculum aims at preparing K12 teachers (and as a result K12 students) for the rigorous tech/STEM learning, specifically in the cybersecurity field. It also prepares them to seek leadership skills and apply their knowledge to real-world problems. This project provides insights into training the trainers whose students can (1) innovate as technologists, and (2) act as social change leaders. In an effort to instill an leadership mindset, the curriculum incorporates industry partners so that the teachers will gain a better understanding of the commercial side of innovation and how it links to a targeted market. This opens a door to bringing the power of the latest in education and leadership to the field of cybersecurity. During the course of this study, there is a possibility of a significant leap towards a more advanced cybersecurity educational methodology using the proposed model.

### 4 Conclusion and Future Work

The proposed curriculum focuses on the analysis of current methodologies for cybersecurity education and leadership in K12 and creating a new model. There is demand for curriculum that extends beyond basic cybersecurity and leverages novel learning science and blended learning delivery methods that can reach more people with the same or better level of learning outcomes. Leveraging a standard set of assessments will further ensure quality as this program is scaled to other agencies or communities. The goal is to change the way K12 teachers think about technology and leadership by
linking them to industry partners, and providing a new model for technical innovation coupled with leadership in cybersecurity. The authors will develop the curriculum tools and learning activity templates that will be tailor-ready for adoption in K12 across the nation, as well as a scalable solution shared with other universities and the public/private educational sectors.

5 References


