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.