2020

Cybersecurity Education Through Technological and Engineering Literacy Standards

Philip A. Reed
Old Dominion University

Steven A. Barbato

Original Publication Citation

Reed, P. A., & Barbato, S. A. (2020). Cybersecurity education through technological and engineering literacy standards. *NICE eNewsletter Winter 2020-2021 Academic Spotlight*, 4 pp. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-enewsletter-winter-2020-21-academic-spotlight

https://www.nist.gov/itl/applied-cybersecurity/nice/nice-enewsletter-winter-2020-21-academic-spotlight

National Institute of Standards and Technology
U.S. Department of Commerce

Information Technology Laboratory (https://www.nist.gov/itl) / Applied Cybersecurity Division (https://www.nist.gov/itl/applied-cybersecurity)

National Initiative for Cybersecurity Education (NICE) (https://www.nist.gov/itl/applied-cybersecurity/nice)

NICE eNewsletter Winter 2020-21 Academic Spotlight

Cybersecurity Education through Technological and Engineering Literacy Standards

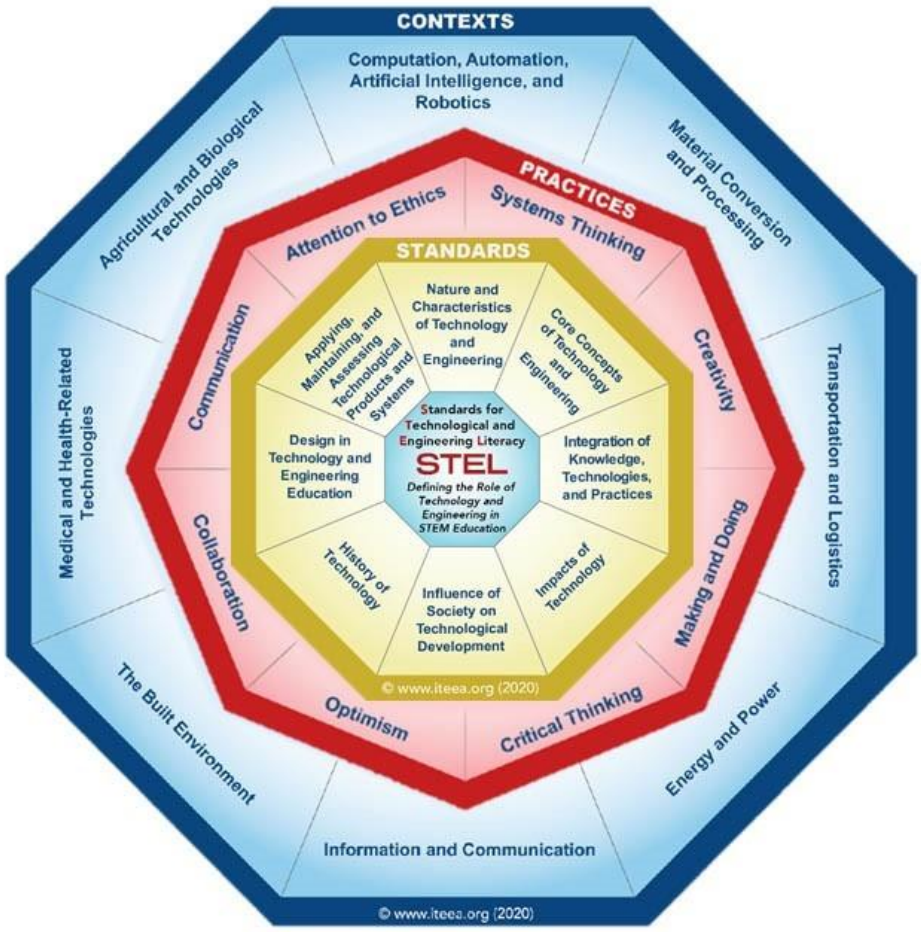
By Philip A. Reed, President, and Steven A. Barbato, Executive Director and CEO, of the International Technology and Engineering Educators Association

A new set of standards for technological and engineering literacy is available to better define a level of literacy expected of learners from pre-K through 12th grade. Focusing on essential knowledge, skills, and dispositions, the set spells out eight core disciplinary standards and eight practices that are widely applicable across a range of technology and engineering contexts, including cybersecurity.

Technology and engineering are pervasive in all aspects of our lives. Every human activity is dependent upon the products, systems, and processes created to help grow food, provide shelter, communicate, work, and recreate. As the world grows more complex, it is increasingly important for everyone to understand more about technology and engineering. The goal is not to make everyone technologists or engineers but to broaden technological and engineering literacy so that people can make informed decisions about technology and better contribute to its design, development, and use.

The increased call for people to enter science, technology, engineering, and mathematics (STEM) occupations is an important reason to study technology and engineering. All occupations require the use of technological products, systems, and processes, and

therefore people with higher levels of technological and engineering literacy are better prepared for the workforce.



Credit: ITEAA

Organization of Standards for Technological and Engineering Literacy (ITEEA, 2020)

A challenge in communicating a clear picture of technological and engineering literacy is that it encompasses a broad area of human activity, one that is constantly evolving. The recently released Standards for Technological and Engineering Literacy: The Role of Technology and Engineering in STEM Education (STEL) (http://www.iteea.org/STEL.aspx) (ITEEA, 2020) distills this broad field into a set of eight core disciplinary standards and eight practices (Figure 1 (https://www.iteea.org/Activities/2142/STEL.aspx#tabs)). The development of STEL was supported by the National Science Foundation and the Technical Foundation of America and is a significant update on ITEEA's Standards for Technological Literacy (http://www.iteea.org/%20Technological_Literacy_Standards.aspx) (2000).

Much like language literacy, scientific literacy, and mathematical literacy, STEL defines a level of technological and engineering literacy that is expected of all learners across the PreK-12 spectrum. It presents the information that students should know and be able to demonstrate to achieve a high level of technological and engineering literacy. In other words, the standards prescribe the outcomes for the study of technology and engineering in Grades PreK-12.

STEL also offers direct connections to the NICE Framework. For example, Table 1 lists the first six NICE Framework Knowledge Descriptions, which are common to all

cybersecurity work roles. Column three lists STEL Standards and Practices aligned to these six NICE Framework Knowledge Descriptions. Ideally, students should study all eight STEL standards and practices. A more detailed cross-mapping of STEL and the NICE Framework demonstrates the other standards and practices that address cybersecurity. In addition, STEL positions cybersecurity across all eight contexts outlined in STEL (see Figure 1 (https://www.iteea.org/Activities/2142/STEL.aspx#tabs)). This is important as cybersecurity is not a monolithic concept. We encourage curriculum developers and teachers to take a more holistic approach when developing cybersecurity curriculum, lesson plans, and courses around these eight contexts. Examples of ITEEA's Engineering byDesign™ Advanced Technological Applications (ADA) course blueprint for units 2 (Cybersecurity) and 4 (Information Technology) (https://www.dropbox.com/s/qzhy8nkuprs7et6/ATA%20Course%20Blueprint-Brief_for_Cyber%282%29_and_Info%284%29Units.docx?dl=0) are available for download.

KSA ID	Description	Connections to *STEL*
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Standard 8: Applying, Maintaining, and Assessing Technological Products and Systems; Practice 1: Systems Thinking
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Standard 3 Integration of Knowledge, Technologies, and Practices; Practice 4: Critical Thinking
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	Standard 2: Core Concepts of Technology; Practice 8: Attention to Ethics
K0004	Knowledge of cybersecurity and privacy principles.	Standard 3: Integration of Knowledge, Technologies, and Practices; Practice 8: Attention to Ethics
K0005	Knowledge of cyber threats and vulnerabilities.	Standard 6: Influence of Technology on Human Progress; Practice 4: Critical Thinking
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Standard 8: Applying, Maintaining, and Assessing Technological Products and Systems; Practice 1: Systems Thinking

Credit: ITEEA

There are an estimated 60,000 U.S. public school secondary technology/engineering teachers, with each state having its own customized technology program. Technology and engineering education are broad in nature and encompass dozens of subdisciplines. These cover a range of critical infrastructure sectors (e.g., energy, transportation, financial services) and comprise a variety of technological focus areas (e.g., biotechnology, information technology, cybersecurity, computer science) to the many engineering sub-specialties, among others. Technology and engineering education, as envisioned in Standards for Technological and Engineering Literacy, provides an effective launching point for continuing study to prepare individuals to work in more specialized areas such as cybersecurity.

The full STEL Document is available for free download at www.iteea.org/stel.aspx (https://www.iteea.org/Activities/2142/www.iteea.org/177416.aspx).

Questions can be sent to ITEEA@ITEEA.ORG (https://www.nist.govmailto:ITEEA@ITEEA.ORG), or call 703-860-2100.

NICE eNewsletter Winter 2020-21 (https://www.nist.gov/itl/applied-cybersecurity/nice/nice-enewsletter-winter-2020-21)

Cybersecurity education and workforce development (https://www.nist.gov/topic-terms/cybersecurity-education-and-workforce-development)
Created December 30, 2020, Updated January 11, 2021