Journal of Cybersecurity Education, Research and Practice

Volume 2024 | Number 1 Article 19

4-8-2024

Comparing Cognitive Theories of Learning Transfer to Advance Cybersecurity Instruction, Assessment, and Testing

Daniel T. Hickey Ph.D.
Indiana University - Bloomington, dthickey@indiana.edu

Ronald J. Kantor
Kantor Consulting, ron@kantorconsulting.com

Comparing Cognitive Theories of Learning Transfer to Advance Cybersecurity Instruction, Assessment, and Testing

Abstract

The cybersecurity threat landscape evolves quickly, continually, and consequentially. This means that the *transfer* of cybersecurity learning is crucial. We compared how different recognized "cognitive" transfer theories might help explain and synergize three aspects of cybersecurity education. These include *teaching and training* in diverse settings, *assessing learning* formatively & summatively, and *testing & measuring* achievement, proficiency, & readiness. We excluded newer sociocultural theories and their implications for inclusion as we explore those theories elsewhere. We first summarized the history of cybersecurity education and proficiency standards considering transfer theories. We then explored each theory and reviewed the most relevant cybersecurity education research; in some cases, we broadened our search to computing education. We concluded that (a) archaic *differential* transfer theories are still influential but have negative implications to be avoided, (b) *constructionist* theories are popular in K-12 settings but raise issues for assessment and transfer, (c) many embrace a *general cognitive science perspective* that can resolve tensions between modern *cognitive-associationist* and *cognitive-constructivist* theories that are popular with innovators, and (d) new *perceptual* and *coordinative* theories have potential worth exploring. These insights should support "generative" cybersecurity learning that transfers readily and widely to future classes, tests, and workplaces. These insights should be beneficial when designing and using cyber "ranges" and other hyper-realistic simulations, where transfer assumptions inform costly design decisions and undergird the validity of performance as evidence of proficiency.

Keywords

Keywords: Cybersecurity education, transfer of learning, assessment, certification, cyber ranges, digital twins.

Cover Page Footnote

This paper was drafted while the first author was supported by a grant from the U.S. National Science Foundation's Improving Undergraduate STEM Education Initiative to Indiana University (Grant #1915498). This work reflects the opinions of the authors and not Indiana University or the U.S. National Science Foundation.

Contrasting Cognitive Theories of Learning Transfer to Advance Cybersecurity Instruction, Assessment, and Testing

Daniel T. Hickey, Ph.D.
Learning Sciences Program
Indiana University
Bloomington, IN, USA
dthickey@iu.edu
https://orcid.org/0000-0001-9146-5089

Ronald J. Kantor, Ph.D.
Kantor Consulting
Charlotte, NC, USA
Ron@KantorConsulting.org

Abstract--The cybersecurity threat landscape evolves quickly, continually, and consequentially. This means that the *transfer* of cybersecurity learning is crucial. We compared how different recognized "cognitive" transfer theories might help explain and synergize three aspects of cybersecurity education. These include *teaching and training* in diverse settings, *assessing learning* formatively and summatively, and *testing and measuring* achievement, proficiency and readiness. We excluded newer sociocultural theories and their implications for inclusion as we explore those elsewhere. We first summarized cybersecurity education history and current proficiency standards. We then explored each theory and reviewed the most relevant cybersecurity education research; in some cases, we broadened our search to computing education. We concluded that (a) archaic *differential* transfer theories are still influential but have negative implications to be avoided, (b) *constructionist* theories are popular in K-12 settings but raise issues for assessment and transfer, (c) many embrace a *general cognitive science perspective* that can resolve tensions between modern *cognitive-associationist* and *cognitive-constructivist* theories that are popular with innovators, and (d) new *perceptual* and *coordinative* theories have potential worth exploring. These insights should support "generative" cybersecurity learning that transfers readily and widely to future classes, tests, and workplaces. These insights should be beneficial when designing and using cyber "ranges" and other hyper-realistic simulations, where transfer assumptions inform costly design decisions and undergird the validity of performance as evidence of proficiency.

Keywords: *Cybersecurity education, transfer of learning, assessment, certification, cyber ranges, digital twins.*

I. INTRODUCTION

Transfer of learning occurs when learning in one setting impacts activity in a different setting. Transfer is vital for cybersecurity education because the threat landscape evolves so quickly (see Whitman & Mattord, 2016). This changing landscape makes it impossible to prepare cybersecurity students or workers for all (or even many) threats they will face. Instead, cybersecurity professionals must transfer what they have learned to those new situations and combine that knowledge with further information. This transfer is particularly crucial during cybersecurity incident responses, which can have extremely high stakes and unfold at breathtaking speed.

Our broad goal is to help cybersecurity educators and educational researchers understand the complex relationships between three aspects of cybersecurity education. *Instruction* includes teaching and training, both in person and online. *Assessment* refers to "everyday" practices that capture evidence of learning from education and training, including summative assessment *of* prior learning and formative assessment *for* supporting that learning. *Testing* concerns measures of readiness and preparedness, as increasingly measured with complex performance assessments, sometimes within hyper-realistic *cyber ranges* and *digital twins*.

Our experience has convinced us that most cybersecurity educators are *generally* familiar with learning transfer and transfer's role in instruction, assessment, and testing. But our experience has also convinced us that many do not understand how transfer theory *connects* instruction, assessment, and testing. For example, most understand that "teaching to the test" is generally wrong, but many don't understand why or how it is wrong. Furthermore, the term "transfer" is used in other potentially confusing ways. For example, Ampel et al. (2020, p. 1) studied *deep transfer learning* from "a source domain using deep neural network architecture," while Gupta and Wolf (2018) studied *knowledge transfer* between cybersecurity researchers and security professionals at the same university.

Our ultimate goal is "systemic validity" (Fredriksen & Collins, 1989), where instruction, assessment, and testing work together to foster a "learning culture" (Shepard, 2000). We contend that such synergy is essential for "generative learning" (Mayer & Wittrock, 1996) that transfers readily and widely to future settings. These future settings include working against cybersecurity threats and responding to cybersecurity incidents. But these also include subsequent education, training, workplace settings, *and* proficiency testing.

A. Methods

Our search uncovered few efforts to establish systemic validity in cybersecurity education. Besides considering professional certifications in college curricula in Tran et al. (2023), we uncovered no systematic explorations of synergistic assessment in cybersecurity education for us to build on. We elected to use an inclusive set of recognized "cognitive" transfer theories to organize a systematic search for the most relevant published research. Along the way, we refined our opinions about that research and implicit and explicit assumptions about learning. Our opinions are partly grounded in two decades of prior research pursuing systemic validity. The first decade focused on computer-based science learning environments (e.g., Hickey et al., 2000, 2003, 2009, and Hickey & Zuiker, 2012). The second (ongoing) decade of research focuses primarily on online learning (e.g., Hickey & Rehak, 2013, Hickey, Chartrand, & Andrews. 2020; Hickey & Harris, 2021) and recently expanded into equity and inclusion (Hickey, Luo, & Lam, in press). The two recent efforts that concerned cybersecurity education (Hickey, Duncan, et al., 2020, Piety et al., 2019-2024) helped motivate us to write this paper.

Our ultimate goal is admittedly ambitious. It calls for several caveats. First, we have excluded (a) transfer theories based on newer situative and sociocultural theories of learning and (b) the implications of all transfer theories for inclusive cybersecurity education that supports diverse learners. We are exploring these issues elsewhere (Hickey & Kantor, in review, in preparation). Our second caveat is that situative transfer theory (e.g., Greeno, Smith, & Moore, 1993; Engle et al., 2012) guided our pursuit of systemic validity. This biases us towards situative theories and their promises for inclusion. But this also provided an objective perspective for comparing cognitive transfer theories, which are far more prevalent in cybersecurity.

As summarized in Appendix 1, we systematically explored the implications of eight transfer theories for designing cybersecurity instruction and assessment. These eight represent the entire range of transfer theories within a broader class of "cognitive" theories of knowing and learning. Compared to newer situative and sociocultural theories, cognitive theories are often characterized as "traditional." This paper emphasizes a traditional "general cognitive science" transfer theory. This theory is best represented by a 1999 report from the National Research Council report entitled *How People Learn: Brain, Mind, Experience, and Schooling.* This report became known as "N I" when the (renamed) National Academy of Sciences, Engineering, and Medicine (NASEM) published the revised "HPL II" in 2017.

Chapter Three of HPL I on "Learning and Transfer" described how (a) transfer assumptions follow from learning assumptions and (b) how learning assumptions follow from knowledge assumptions. These connections between knowledge, learning, and transfer are very direct. This is because the nature of knowledge dictates how that knowledge is learned and, therefore, how that learning transfers. These assumptions have strong *implications* for designing instruction, assessing learning, and testing proficiency. This difference between assumptions and implications is crucial for our goals. Educational practice is influenced by other factors such as cost, efficiency, and tradition. These factors often overrule assumptions about knowing, learning, and transfer. These issues are crucial for coherent theory when pursuing systemic validity.

While seldom cited in cybersecurity education and only modestly cited in computing education, HPL I & II are extremely influential more generally. They are "consensus study reports" that carefully capture the consensus of leading experts on significant scientific questions *at that time*. (NASEM, 2024). Consider, for example, that the subtitle of HPL II, two decades later, is *Learners, Contexts, and Cultures.* This subtitle and a new chapter on context and culture document a broad shift among cognitive scientists toward newer sociocultural theories. Furthermore, the presence of a transfer chapter in HPL I and the absence of a transfer chapter in HPL II suggests that this shift towards sociocultural theories undermined the prior cognitive consensus on transfer.

However, sociocultural theories have had little impact on cybersecurity education and only limited impact on computing education (e.g., NASEM, 2021). We show that the general cognitive science view in HPL I is most consistent with the current transfer assumptions among cybersecurity educators and educational researchers. Hence, we believe a general cognitive science perspective may be an ideal starting point for understanding how transfer connects cybersecurity instruction, assessment, and testing.

We also explore the implications of seven other more specific cognitive transfer theories for designing instruction and assessing learning. We first document the potentially harmful influence of historic *differential* theories and the potentially confusing influence of modern *constructionist* theories. After relatively extensive consideration of the general cognitive science perspective, we review how cybersecurity innovators have applied modern *associationist*, *constructivist,* and *socio-constructivist* theories. Finally, we consider how innovators might use emerging *perceptual* and *coordinative* theories.

We first explored and then briefly summarized the evolution of cybersecurity education. For all eight theories, we attempted to locate and review the best examples of research on cybersecurity instruction and assessment using those theories. In some cases, we turned to computing education more broadly. We also explored the implications of each theory for cybersecurity proficiency testing, with a particular focus on performance-based measures and sophisticated simulations and cyber ranges. However, such testing raises issues of validity, reliability, bias, cost, and psychometrics that quickly exceed our scope and space. While we tried to provide valuable new insights for designing and using these new measures, our primary audience is educators and designers who create instruction and assessments and researchers who study those practices.

II. EVOLUTION OF CYBERSECURITY ED

Compared to cybersecurity, the cybersecurity *education* field is much smaller. However, this smaller field has grown steadily in response to increased workforce requirements due to the growing number and economic impact of cyber threats (Caelli, 2020). Most computer science degrees required at least one cybersecurity course by 2013, and two-year, four-year, and graduate cybersecurity degree programs have grown steadily (Cabaj et al., 2018). Austin (2020) and Daimi and Francia (2020) present many relevant contributions.

The steady expansion of cybersecurity education in universities mirrors the growing U.S. federal interest. Following notable developments in 2008 in the George W. Bush administration (*Comprehensive National Cybersecurity Initiative*, 2023) and in 2009 in the Obama administration (The White House, 2010), the National Initiative for Cybersecurity Education (NICE) was established in 2010 by the National Institute of Standards and Technology (NIST).[1] NICE organizes much of its work around the *NICE Framework* which was published in 2017 and revised in 2020 and is now called the *NICE Workforce Framework for Cybersecurity*. The 2020 NWFC includes 31 specialty areas, 53 work roles, 176 abilities, 374 skills, 630 knowledge descriptions, and 1007 tasks. As will be shown, this specification of numerous "KSAs" ("knowledge, skills, and abilities") has significant implications for education. This is because most KSAs are on the lower part of Benjamin Bloom's well-known hierarchy of increasingly sophisticated learning objectives (e.g., Dupuis, 2017). This structure implies that higher-order "critical thinking" skills consist of organized "stacks" of these more basic skills. This assumption has direct implications for instruction, assessment, and testing. As we will show, this assumption is (a) entirely consistent with associationist transfer theories, (b) partly consistent with general cognitive science theories, and (c) antithetical to constructivist theories.

Alongside academic and federal efforts to support cybersecurity expertise, five industry associations under the leadership of the Association for Computing Machinery (ACM) established the Joint Task Force on Cybersecurity Education in 2015.[2] The task force described the field as "an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries" (ACM, 2017, p. 16). It is this "context of adversaries" that makes transfer so central to cybersecurity education. A hallmark of cybersecurity expertise is captured by the skill of *adversarial thinking*, where the cybersecurity professional must get into the "mindset" of attackers to stay ahead of the evolving threat landscape (Hamman & Hopkinson, 2016; Thompson et al., 2018).

Adversarial thinking is one of six "crosscutting concepts" in the *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity* that the Joint Industry Task Force published (ACM, 2017). Illustrating one of our central points, these crosscutting concepts higher on Bloom's taxonomy suggest a different emphasis than the more specific KSAs in the NCWF and are consistent with constructionist and constructivist transfer theories. Crosscutting concepts are also prominently featured in the Next Generation Science Standards that are reshaping K-12 science education in the US. We explore the distinction between KSAs and crosscutting concepts and other similar issues in cybersecurity education for eight transfer theories in the sections that follow.

A. The Emergence and Importance of Cyber Ranges

While space does not permit full elaboration, we are particularly interested in instruction, assessment, and testing using increasingly popular cyber "ranges" and "digital twins" (e.g., Beauchamp & Matusovich, 2023; Bohm et al., 2021). These hyper-realistic simulations can be quickly adapted to teach, assess, and test for new threats. This adaptability is why many argue that they provide more valid ways of teaching and assessing workforce readiness and military preparedness (Bécue et al., 2018). However, sophisticated features make ranges relatively expensive to build, operate, and maintain (Naponen et al., 2022). Massive numbers of users partly mitigate these costs. But in most cases, emphasizing one goal or feature over another or making significant revisions represents a substantial investment. Consider, for example, how the NICE summarized a core tension in *Cyber Range: A Guide*:

> Individuals and organizations must find a balance among three competing interests – cost, practicality, and reality. Teaching or training individual skills may even benefit from a less realistic scenario to allow the trainer and student to focus on the skill to be mastered. Integrating that skill into more realistic environments can come later in the training cycle. (2018, p. 8)

As will be shown, teaching specific skills in isolation from a more realistic environment raises a central debate about instruction that emerged in the cognitive "revolution" of the 1970s and that continues today. This means that *how* innovators use cyber ranges and digital twins is likely as important as *if* they use them. We aim to offer new theoretical and practical guidance for designing and using these transformative technologies to teach, assess, and (possibly) certify cybersecurity expertise.

III. DIFFERENTIAL THEORIES OF LEARING AND TRANSFER

The practices of some cybersecurity educators and the design of most cybersecurity certification tests are consistent with *differential* transfer theories. These theories emerged historically in the early 20th century in efforts to uncover individual differences in presumably stable traits, such as the aptly named intelligence *quotient* (I.Q.) Differential theorists defined learning and transfer entirely by the test items used

[1] https://www.nist.gov/itl/applied-cybersecurity/nice

[2] https://cybered.acm.org/

to "differentiate" test takers. Most learning and cognitive scientists have abandoned differential theories. But HPL I reminded us that differential theories continue to influence via "elaborate statistical machinery was developed for determining the separate factors that define the structure of intellect" (NRC, 1999, p. 61-62). Standardized achievement and proficiency tests still use key elements of this statistical machinery. Because certification tests are so important in cybersecurity, the idea that "learning" is whatever a test measures still influences cybersecurity education in two important ways. The first is via what some call "folk pedagogy."

A. Differential Theories and Folk Pedagogy

Most cybersecurity educators came to their role via their expertise in cybersecurity and have relatively little training in scientific learning theories. We have observed that many (but certainly not all) such educators embrace learning and transfer ideas loosely consistent with differential theories. This embrace means that they likely assume that (a) assessments and tests capture meaningful knowledge, (b) higher scores are better, and (c) higher scores are better by any means necessary except for cheating (see Sanders et al., 2017).

These assumptions are problematic in part because different individuals can attain the same test score by very different means. For example, compare a learner who attains a passing score on a given test using a commercial test preparation program that guarantees passage (e.g., *TrainingCamp*, 2024) with a graduate of a high-quality degree program that ignores proficiency tests. Arguably, differential assumptions underpin the "folk pedagogy" (Olson & Bruner, 1996) that drives large swaths of cybersecurity education and assessment. Presumably, because approaches are based on archaic theories, we were unable to locate empirical or narrative evidence of differential instruction and assessment. However, we are confident that most readers have witnessed such assumptions in practice (see Padmos, 2018).

The fundamental problem with differential instruction and assessment is that certification tests must transform cybersecurity knowledge into the numerous relatively specific associations represented by each test item. Directly teaching students those associations boosts scores artificially, undermines validity, and results in knowledge that is unlikely to transfer beyond answering those items. Directly teaching more general test-like associations (i.e., not necessarily on a targeted test) should result in scores that more accurately estimate transferable knowledge when comparing test takers. However, the resulting knowledge is still likely fragile and disorganized and, therefore, less likely to transfer.

It is worth noting that the cognitive processes used to answer conventional test items are debatable and debated (see Mislevey, 1996; Pellegrino & Glaser, 1982). Professional item writers create "best answer" items where sophisticated reasoning is presumably necessary to identify which of several partially plausible answers is the most correct answer. However, these insights likely have little impact on folk pedagogy and assessment.

B. Constructionist Theory and General Transfer of General Skills

The second way differential theory lives on is more complex than folk pedagogy and likely confusing. This influence comes from *constructionism* (Kafai & Resnick, 1996). Mostly in K-12 schools, cybersecurity education embraces constructionism via "block-based" programming tools like MIT's *Scratch* and Google's *Blockly* that let learners "program" without learning code (see Appendix 1). For example, the *Cybersecurity Lab* from the Corporation for Public Broadcasting (2022) uses Blockly to teach middle and secondary students about personal cybersecurity (see also Yett et al., 2020). Block-based programming focuses on general computing concepts (such as the idea of *recursion,* where a function calls on itself) rather than the actual code used to program computational functions. Constructionism also influences cybersecurity education via *computational thinking* (CT, Yadav et al., 2018; Yett, 2020). CT is strongly associated with block-based programming. But is also used in diverse cybersecurity education contexts, such as teaching liberal arts majors (Mountrouidou et al., 2018), K-12 teacher education (Burrows et al., 2022), and aspects of high school Advanced Placement computer science courses (Mishra et al., 2017).

In addition to teaching very general concepts, education with block-based programming and computation thinking usually avoids assessing and testing specific skills. Instead, block-based programming typically relies on completed projects and portfolios as evidence of learning (e.g., Grover et al., 2017). This is because constructionism assumes relatively general transfer of these general thinking skills. This theory of transfer is known as *formal discipline*. As featured in newly resurgent "classical education" (e.g., Williams, 2022), formal discipline theory assumes that traditional subjects like Latin and geometry make students more logical and disciplined and that these very general skills transfer readily and widely. Formal discipline theory is consistent with Jean Piaget's influential theories of the general "stages" of human development (e.g., 1954) and with the many "thinking skills" programs that emerged in the 1980s. As influentially summarized in HPL I, numerous studies of thinking skills programs (most notably the influential LOGO graphical programming language from Papert, 1980) showed that such general thinking skills only transferred to very similar problems and did not transfer to different problems or achievement tests. These studies led most cognitive scientists to shift towards more domain-specific forms of knowing and learning (Glaser, 1984). However, a more subtle version of formal discipline transfer lives on in constructionism, computational thinking, and classical education.

It is beyond the scope of this paper to review the continuing debate on whether general competencies learned in block-based programming or CT transfer to conventional

coding (see Zhang & Nouri, 2019). We remind readers that (a) the debate exists and endures, (b) the debate is partly rooted in how coding proficiency is assessed, and (c) the general skills learned in block-based programming and CT are much harder to assess than more specific text-based coding skills. It is also worth noting that the renowned constructionist theorist Yasmin Kafai recently introduced "computational literacy" (Kafai & Proctor, 2022) to incorporate newer sociocultural theories into CT. We agree with proponents that block-based programming and CT can introduce younger and more diverse students to cybersecurity and help motivate their learning. But we also agree with computer science educators who worry that the general computing knowledge gained independently of more specific coding skills won't transfer to education once coding becomes necessary (see Pappano, 2017).

IV. GENERAL COGNTIVE SCIENCE PERSPECIVES

Many current innovations in cybersecurity education appear consistent with the general cognitive science perspective in HPL I introduced above. These innovations include *active* learning (Ibrahim & Ford, 2021), *experiential* learning (e.g., Konak, 2018; Payne et al., 2021), *collaborative* learning (Konak & Bartolacci, 2016), and most cyber ranges (e.g., Karjalainen & Kokkonen, 2020).

The cognitive revolution in the 1970s laid the groundwork for the more specific theories of transfer explored in other sections. As illustrated by HPL I, some cognitive scientists and many educational psychologists and learning scientists do *not* adhere to one of the more specific transfer theories. As summarized in Appendix 1, a more general perspective on transfer sidesteps the nagging debate over teaching specific skills (in associationist approaches) vs. general skills (in constructivist approaches) by starting with specific skills and building to more general skills and by assessing both specific and general problem-solving skills.

A useful reference for the general cognitive science perspective is Mayer and Wittrock's (1996) handbook chapter entitled *Problem Solving Transfer.* They inclusively label their general transfer theory *cognitive science*. This broad framing allowed them to summarize research on "teachable aspects of problem-solving." This includes *teaching basic skills, teaching for understanding, teaching by analogy,* and *teaching thinking skills.* They subtitled their general transfer theory *metacognitive control of general and specific skills.* This further framing emphasized metacognitive control of one's own cognitive processes, which had emerged as a major strand of research in educational psychology research by that time. The chapter established the theoretical groundwork for Mayer's influential theory of *multimedia learning* (Mayer, 2005). Multimedia learning is organized around initial basic skills instruction, building up to practice with larger, more complex problem-solving practices. Multimedia learning creates increasingly expert mental models by combining words and images, often using computer-based visualizations and simulations, all towards valid assessments of problem-solving transfer (using different problems than those used in instruction). Consistent with the associationist theories below, multimedia learning theory worries about "cognitive load," where "supplemental" material interferes with learning the targeted knowledge. The practical implication is that competing constructionist and constructivist approaches that *introduce* targeted concepts within broader problem-solving contexts or fictional narratives present an excessive cognitive load that overwhelms most learners.

Multimedia learning theory has influenced computing education research and is particularly pronounced in the work of the influential cluster of computing education researchers that emerged at the Georgia Institute of Technology (e.g., Guzdial, 2010; Margulieux, 2016). While we found some considerations of cognitive load (e.g., Bernard et al., 2021), we found surprisingly few references to Mayer's theories in cybersecurity education. We suspect that multimedia learning theory has far more relevance than the research literature suggests. For example, multimedia learning appears immediately relevant to the balance described above in designing cyber ranges. However, as we show next, the general cognitive science transfer assumptions at the core of multimedia learning theories have been taken up independently in cybersecurity education.

A. Analogical Transfer in Cybersecurity Education

General cognitive science views of problem-solving transfer and Mayer's multimedia learning theory focus primarily on *analogical transfer.* Analogies are abstract representations of concepts that form the backbone of most cognitive theories and can represent specific concepts *and* more sophisticated reasoning. We believe that a general perspective, multimedia learning theory, and analogical transfer have tremendous untapped potential for cybersecurity education. Indeed. These may be the ideal starting point for many innovators aiming to align cybersecurity instruction, assessment, and testing.

Mayer and Wittrock (1996, p. 55) summarized the three cognitive conditions necessary for analogical transfer. These included *recognition* (recognizing that analogical reasoning learned in the initial environment is relevant to solving the problem in the transfer environment), a*bstraction* (learning the general principles or strategies in the initial environment), and *mapping* (mapping the learned general principle or strategy to the new problem in the transfer environment).

The general cognitive science perspective and analogical transfer appear consistent with many high-quality university-based cybersecurity education programs. Prerequisite basic skills are taught and learned to fluency using tell and practice (T&P), where lectures and readings are followed by hands-on laboratory practice. These activities are followed by "worked examples" or other "constraint removal" methods that let students focus on larger problem-solving tasks without the attention-demanding requirements associated with basic skills (e.g., González-Torres et al., 2020). In this approach, cybersecurity instruction gets more and more sophisticated as fluency with basic skills develops, with an

increased focus on teaching by analogy and practice solving more complex problems. Margulieux et al. (2021) offer a carefully designed study that systematically compared analogical transfer methods with a range of other approaches in computing education.

One open question for instruction raised by Mayer and Wittrock (1996) concerns metacognition. Cognitive scientists have generated a diverse range of "active" (versus "passive") learning strategies to promote the transfer of problem-solving instruction. While we found little discussion of metacognition in current cybersecurity education research literature, there is a strong push towards using more active learning strategies and introducing them earlier in cybersecurity programs (see Dark, 2014). This trend is significant because giving students practice managing their cognitive processes is a central goal of active learning strategies. At a general level, these active learning strategies include Sternberg's (1990) strategies for *selective encoding, selective combination,* and *selective comparison.* Many more specific classes of active learning models have emerged over the years. In cybersecurity, these include *integrative learning* (Abraham & Shih, 2015) and *high-impact practices* (Payne et al., 2021).

Mayer and Wittrock (1996) and multimedia learning theory also endorse *discovery learning*, which is more consistent with the constructivist theories explored next. Reflecting concerns over cognitive load, they do not encourage "unguided" learning until learners have developed substantial fluency with underlying concepts and skills. Indeed, many cybersecurity education programs only include discovery-oriented and inquiry-based learning at the end of coursework. These can range from more structured "capstone" projects (Lesco, 2019) to more elaborate competitions (e.g., Bowen et al., 2022) and cyber-ranges.

B. "Authentic" Cybersecurity Instruction in General Cognitive Science Approaches

Central to most general cognitive science approaches, capstones, competitions, and ranges is the value of "authentic" learning environments. The title of a 2021 NASEM consensus study report on computing education captures the broad support for authentic learning: *Cultivating Interest and Competencies in Computing: Authentic Experiences and Design Factors.* The report defined authentic activities as follows:

> Authentic, open-ended learning activities—through project- or problem-based learning and makerspaces—have been offered as an approach to support broader access to STEM learning and can catalyze interests and learning in computing. These open-ended experiences are "authentic" in the sense that they are designed to reflect the practices of the discipline; that is, they are close approximations to the work that a STEM professional would engage in. In addition to approximating the work of the professional, there has been increasing attention to designing authentic STEM experiences so that they are connected to real-world problems learners' care about and the challenges they face. (NASEM, 2021, p. 11)

As a consensus study, the report does not specify how authenticity should be incorporated into instruction and assessment. However, the report defined authenticity in a way that helps clarify one of our key goals across our set of papers. The report distinguished between "professionally authentic" and "personally authentic" experiences. More consistent with all cognitive transfer theories, professionally authentic activities "exhibit features of problem-solving, creation, experimentation, and inquiry that mirror or are directly connected to the culture, practices, and communities of computing professionals" (2021, p. 30). The authenticity of such practices is usually defined by instructors and experts rather than learners; such professionally authentic experiences are well represented in cybersecurity education (e.g., Giboney et al., 2021) and are central to the K-12 GenCyber summer camps sponsored by the U.S. National Security Agency and the National Science Foundation (Payne et al., 2016). The ten *first principles of cybersecurity* that organize the GenCyber program (e.g., *domain separation, least privileges modularity,* etc.) present a detailed framework for offering professionally authentic experiences to younger learners.

Reflecting the goal of inclusive computing education and the influence of newer sociocultural theories of learning and transfer (as emphasized in HPL II), the 2021 NASEM computing report defined *personally* authentic experiences as "personally or culturally meaningful in the mind of the learner" (p. 30). Significantly, the report argues that any tension between professional and personal authenticity is caused by placing them on opposite ends of a single continuum. The report suggests instead that each represents its own continuum and that a given experience can be more or less personally and/or professionally relevant on each continuum. Hickey and Kantor (in review) explore personally authentic experiences and their relationship with situative transfer theory, while Hickey and Kantor (in preparation) explore the cultural aspects of personally authentic experiences and their implications for inclusive cybersecurity education. Our arguments across all three papers are that (a) authenticity is a central issue in generative cybersecurity learning, (b) simplistically characterizing learning experiences as "authentic" without specifying a theory of learning and transfer is imprecise and unproductive, and (c) that personally authentic experiences are likely necessary to accomplish widely-held goals for supporting diverse cybersecurity learners. These arguments and concerns over authenticity are particularly significant given the relatively massive investment now underway in hyper-realistic cyber ranges.

C. Assessing Analogical Transfer of Cybersecurity Learning

Mayer and Wittrock (1996) influentially argued that assessing meaningful analogical transfer required "actual" problem-solving and that "traditional" tests cannot capture transfer of more sophisticated problem-solving skills. These assumptions underly many calls for "alternative" assessments and fuel concerns about the validity of relatively efficient

multiple-choice tests as evidence of likely transfer, compared to the more complex problem-solving assessments. Nonetheless, most "alternative" assessment formats are relatively laborious for students and educators and costly for institutions. Furthermore, as cautioned by Messick (1994), the assumption that "authentic" performance assessments necessarily generate more valid evidence of competency (and likely transfer) is often and easily undermined by overly aligning instruction to assessment problems. We contend that this is a massive issue that cyber ranges need to address to accomplish their stated goals for assessment and testing.

A useful general cognitive science assessment resource is another consensus study report entitled *Knowing What Students Know* (NRC, 2001). The report introduced a helpful framework called the *assessment triangle.* The triangle has helped many appreciate that all educational assessments involve the interplay between (a) an underlying "construct" of competence (i.e., a theory of competence beyond the assessment itself), (b) a task or activity that can be observed or scored, and (c) a way of scoring and interpreting individual responses. The report convinced many that all three require a single theory of cognition to function coherently (see also Pellegrino et al., 2016; Pellegrino, 2018)

The 2001 NRC assessment report summarized relevant research on assessment principles such as validity, reliability, and bias and provided helpful guidelines when assessing for formative, summative, and evaluative purposes. Perhaps most importantly, the report provides a coherent framework for designing and implementing assessments that generate valid evidence of transfer within the constraints presented by typical educational contexts. This includes pragmatically adapting more specific theories of learning and transfer to assess more specific forms of learning and understanding how and why different kinds of instruction should transfer (or not) to educational assessments and externally developed competency tests. As with multimedia learning, we were disappointed to find no substantive considerations of this report in cybersecurity education.

In summary, a general cognitive science perspective, multimedia learning theory, and analogical transfer are promising starting points for many cybersecurity educators and educational researchers pursuing synergy between instruction, assessment, and testing. These ideas seem like a useful starting point for (a) helping many cybersecurity educators move beyond problematic applications of differential theory and (b) helping cybersecurity innovators to move beyond unproductive theory-free appeals to "active learning," "authentic instruction," and "alternative assessment." When coupled with the assessment guidelines in NRC (2001), such instruction is likely to be more generative than many existing practices.

V. OTHER MORE SPECIFIC COGNITIVE THEORIES

The cognitive revolution spawned many research programs exploring more specific transfer theories beyond those above. Space limitations restrict what we can present here. For further elaboration, we refer readers to the landmark volume edited by Detterman and Sternberg (1993), the journal strands edited by Lobato (2006) and Engle (2012), the special issue edited by Goldstone and Day (2012), and the volume edited by Mestre (2006).

A. Cognitive-Associationist Theories

Associationist theories of transfer are embodied in cybersecurity innovations such as *personalized learning* (Chowdhury & Gkioulos, 2023; Deng et al., 2018), *adaptive learning* (Vykopal et al., 2022), *cognitive tutors* (Bier et al., 2011), *competency-based education* (Tobey et al., 2018), most commercial test preparation programs (e.g., Conklin, et al., 2022; CBT Nuggets, 2024), and many massively open online courses (MOOCs, Laato et al., 2020). As the label implies, associationist theories characterize learning and transfer in terms of associations between numerous "fragments" of knowledge. In earlier behavioral-associationist perspectives and associated "mastery learning" schemes, these fragments were stimulus-response associations between external (i.e., not cognitive) stimuli and behavioral responses (Skinner, 1958). Within the cognitive revolution, some theorists (most notably John Anderson, e.g., 1982) maintained this focus on smaller associations but supplanted behaviorism's stimulus-response associations with cognitive associations. As summarized in Appendix 1, associationist perspectives diverge from general cognitive science perspectives by assuming that *all* complex competencies can and should be broken down into specific associations. These associations are then taught in carefully structured sequences. Mastery of these associations can be efficiently assessed with multiple-choice items. This allows self-paced "personalized" learning where learners individually progress as they master these specific competencies.

Associationist theorists have long resisted the concern that teaching highly specific associations will fail to result in proficiencies like adversarial thinking at the top of Bloom's taxonomy. Rather, associationist perspectives strongly assume that such higher-order knowledge consists of organized hierarchies of these more specific associations. (Koedinger et al., 2012) Associationist theories are *reductionist* (complex concepts consist of these smaller fragments) and *additive* (these fragments readily assemble into an accurate representation of more complex knowledge). When individuals engage in sophisticated problem-solving, associationist theory assumes that they use the necessary lower-level knowledge and skill components. Hence, associationist theories are often described as "bottom-up," as opposed to the "top-down" constructivist theories.

If learning is seen as acquiring numerous associations from the environment, those associations are what transfer to a new environment. Therefore, associationist transfer is relatively unproblematic. As represented by the *identical elements* theory (Singley & Anderson, 1989), specific cognitive associations of *declarative, procedural,* and *conditional* knowledge formed in a learning environment are assumed to transfer readily so long as identical associations

in the learning environment are needed in the transfer environment. Associationist representations of knowledge and learning are much easier to model using computers than other representations. This feature has made associationist theory extremely influential in instructional technology, including the cybersecurity examples listed above. A fine-grained analysis of competency enables computers to continuously update a digital model of each learner's knowledge; the computer uses this model to estimate what each learner is most ready to learn and delivers instruction accordingly.

B. Cognitive-Associationist Instruction

Key features of associationist instruction are (a) highly structured activities that efficiently present to-be-learned knowledge, (b) clear goals with reinforcement and feedback, and (c) a sequence from smaller elements to larger compositions of those elements (Greeno et al., 1996, p. 27; see Robins et al., 2019). Readers should note that NICE's NCWF does *not* explicitly recommend or endorse associationist instruction and assessment for its hundreds of KSAs. However, the NCWF work roles for *Cyber Instructional Curriculum Developer* and *Cyber Instructor* provide clues about their implicit assumptions. The work roles include knowledge of Gagné's (1985) *Nine Events of Instruction* that specify "direct instruction" that exposes students to carefully structured sequences of very specific elements of the curriculum.

Perhaps the most relevant influence of associationist theory for intended readers is via increasingly popular competency-based education (CBE). CBE is fully embraced by two online "megaversities" (Western Governors University and Southern New Hampshire University), which are among the top annual producers of cybersecurity graduates. CBE is employed in many other online cybersecurity degree programs and enjoys broad support from leading private educational philanthropies (e.g., Bill and Melinda Gates Foundation, 2011; Chan Zuckerberg Initiative, 2017; Lumina Foundation, 2024). CBE is very assessment-driven and typically allows students to "test out" of courses. In cybersecurity education, CBE in cybersecurity education is perhaps best illustrated by the National Cyberwatch Center. The center's aptly titled *Cybersecurity Skills Journal* (CSJ) "seeks to integrate and expand the methods, processes, and evidence of effective practices which underlie skilled performance" and "focuses on valued measured results; considers the larger system context of people's performance; and provides valid and reliable measures of effectiveness." (Cybersecurity Skills Journal, 2024). The CSJ Editor-in-Chief and colleagues published an article whose title referenced associationism's enduring (and often acrimonious) debate with constructivism: "Competency is Not a Three-Letter Word." It asserted that "competency is a complex, multidimensional construct which *must be decomposed* to fully understand" (Tobey et al., 2018, p. 32, emphasis added).

C. Cognitive-Associationist Assessment

Assessment of associationist learning is relatively unproblematic because evidence that learners have formed targeted associations is presumably evidence of knowledge that is likely to transfer to subsequent settings. Because selected-response tests can be easily automated, testing firms have long been able to use computers to draw from relatively massive banks of test items. The advent of computer-adaptive testing has dramatically increased efficiency (by estimating proficiency with increasing accuracy across items and only offering items around that estimate). These developments let testing professionals and organizations create standardized tests that efficiently estimate each test-taker's relative knowledge of a domain with astonishing reliability. Readers should note that the presence or use of multiple-choice items does *not* necessarily imply an associationist perspective or that the test only measures specific associations. To reiterate the reasoning processes that test takers use to answer sophisticated "best answer" items created by professional test developers are debatable and debated. Just as we discourage simplistic appeals to "authentic" instruction and "alternative" assessments, we discourage simplistic dismissals of conventional professionally developed proficiency tests as evidence of transferrable knowledge. For the reasons we elaborate below, many measurement professionals argue that such tests are necessary to make efficient and accurate comparisons of knowledge across takers.

D. Summary of Cognitive-Associationist Approaches

In summary, cognitive associationist perspectives suggest (a) breaking competency down into relatively specific elements, (b) directly presenting learners with very carefully constructed sequences of these elements, and then (c) directly assessing those elements. While skeptics question whether isolated elements readily transfer and reassemble as needed, this decomposition directly supports adaptive tutoring systems and competency-based education and indirectly supports most cybersecurity testing practices

E. Cognitive-Constructivist and Socio-Constructivist Theories

As embodied by *inquiry-based* learning (e.g., Alexander et al., 2023; Konak, 2018) and many variants of *collaborative* learning (e.g., Konak & Bartolacci, 2016) and *problem-based learning (*e.g., Cusak, 2023), constructivist perspectives are prominent in cybersecurity education innovations. Workman (2021, p. 2) reported survey results that found "wide use of a dialectical-contextual social constructivism method in which classroom lectures and team-based tasks are paired with laboratory exercises." Constructivist perspectives are further embodied in the crosscutting concepts such as adversarial thinking in the CSEC2017 standards and Dark's (2015) notion of a "cybersecurity mindset."

The distinction between constructivist approaches to instruction and the more general cognitive science approach is potentially confusing. The distinction is perhaps most apparent in the way that instruction is *framed* (i.e.,

contextualized). Constructivist approaches to cybersecurity education emphasize crosscutting concepts such as adversarial thinking from the *outset*, using complex real-world contexts to frame more specific content. This framing sets aside concerns with cognitive load. This is because these perspectives primarily (if not exclusively) characterize knowing, learning, and transfer using higher-order cognitive or conceptual structures. Constructivist perspectives assume that humans create these structures to make sense of patterns in the environment and solve problems. From a constructivist perspective, the higher-order mental "schema" constructed when solving problems in the learning environment are what individuals transfer and use to solve problems in subsequent transfer environments (e.g., Reed, 2020).

Many influential constructivist approaches (e.g., Cognition and Technology Group at Vanderbilt, 1990; Hmelo-Silver, 2004) involve more social interaction and collaboration and are often characterized as *socio-constructivist* (Amieh & Asl, 2015) (See Appendix 1). Socio-constructivist approaches are often juxtaposed with passive, isolated learning. For example, Shivapurkar et al. (2020) compared cybersecurity problem-based learning with a "traditional lecture-based approach followed by laboratory exercises," which "fails to provide students with an opportunity to completely explore the multi-faceted and ill-defined problems prevalent in the real-world cybersecurity scenarios" (p. 1). Other noteworthy socio-constructivist cybersecurity innovations include *playable case studies* from Giboney et al. (2021) and the *collaborative learning laboratory* from Murphy et al. (2014).

F. Constructivist Transfer as Preparation for Future Learning

Preparation for future learning" (PFL) emerged in an influential socio-constructivist program of transfer research led by John Bransford and Dan Schwartz (e.g., 1999; Bransford co-chaired the committee that produced HPL I). PFL offers a helpful starting point for thinking about transfer and assessment in cybersecurity education that extends to other theories as well. Bransford and Schwartz pointed out that most education prepares students for future classes or training. This common understanding of PFL holds for most cybersecurity education, where students learn basic concepts in introductory classes to prepare for more advanced classes. For example, many students learn introductory cybersecurity concepts (e.g., *hashing* and *threat actors*) in lower-division computing classes. The classroom assessments used to assign grades in the introductory course should estimate preparedness for future learning that builds on those concepts in the more advanced classes. The similarity between instruction and assessments is crucial. If the instruction is too similar, the assessment can't capture valid evidence of preparation for future learning.

But PFL is also relevant to cybersecurity workplace learning. Because of the ever-changing threat landscape, the on-the-job learning of working cybersecurity professionals should prepare them to learn how to respond to new threats in the future. We suspect that PFL might be quite relevant when organizing and studying mentoring and supervision of entry-level cybersecurity professionals.

G. Assessing Constructivist Learning

Constructivist theories have influenced most prior "waves" of assessment reform in education (e.g., Black & Wiliam, 1998; Wolf et al., 1991). Constructivist perspectives suggest "assessments of extended performance" and "crediting varieties of excellence" (Greeno et al., 1996, p. 39) with "alternative" formats such as open-ended problem-solving tasks and extended performance assessments (Wiggins, 1998; Hickey et al., 2000; Hickey & Zuiker, 2012). Such formats include a relatively small number of items that traditionally must be scored by humans and that present challenges to traditional psychometric methods (but see Frezzo et al., 2010, and Snow et al., 2019).

We found surprisingly little research on cybersecurity performance assessment in the research literature (constructivist or not, see Gallagher, 2016). A 2013 NRC workshop report entitled *Professionalizing the Nations Cybersecurity Workforce* reported that:

> One issue that is listed in the statement of task but is not addressed in this report is the question of approaches to performance assessment. The reason for this omission is simple: the committee did not hear about this point at the workshops it convened. The committee believes that this issue will merit more attention in the future as professionalization measures are implemented and refined. (p. ix)

As with the general cognitive science perspective, we believe that Knowing What Students Know (NRC, 2001) offers cybersecurity educators useful guidance for assessing constructivist learning.

We remind readers that most constructivist theorists question the validity of scores from traditional assessments as evidence of transferable knowledge. For example, Bransford and Schwartz (1999) criticized prior research on analogical transfer for its reliance on "sequestered problem solving" assessment. They argued that with sequestered assessments, "there are no opportunities for [students] to demonstrate their abilities to learn to solve new problems by seeking help from other resources such as texts or colleagues or by trying things out, receiving feedback, and getting opportunities to revise" (p. 68).

In many cybersecurity educational contexts, the constructivist "do no harm" stance towards traditional testing (Lamon et al., 2013) seems insufficient given the immense pressure attached to certification tests and the widespread dissatisfaction with the workforce readiness of graduates from cybersecurity degree programs (Lewis, 2019; Marquardson, & Elnoshokaty, 2020). Given the rapid expansion of cyber ranges, performance assessment seems like a crucial issue for further investigation. We worry that constructivist innovators will ignore the concerns that pioneering validity theorist Samuel Messick (1994) raised in the first major wave of U.S. K-12 assessment reforms.

Messick argued that *construct irrelevant easiness* (i.e., "teaching to the test") is often a greater problem with performance assessment—and is often harder to detect. This is because of the necessarily limited number of problems on a given assessment compared to multiple-choice tests impacts the crucial *alignment* of instruction and assessment. Alignment between instruction and performance assessments must be established interpretively by systematically comparing the two (Haertel, 1999; Hickey & Pellegrino, 2005); in contrast, the alignment of instruction and traditional test can be established empirically, where the relatively large number of items reduces the likelihood that problems used in instruction will also be used multiple items in the assessment (see Stecher & Klein, 1997; Klein et al., 2007)

H. Summary of Constructivist Approaches

In summary, constructivist transfer theories support a range of innovations in cybersecurity instruction and assessment. Most set aside concerns with cognitive load and frame instruction from the outset using authentic problem-solving contexts. These contexts are typically designed or selected by experts or professionals to best help learners develop more expert problem-solving skills. While these skills are more general than the specific competencies in associationist theory, they are assumed to be specific to domains and, therefore, unlikely to transfer to different domains. With problem-based learning and other related innovations, there are plenty of applications of constructivist theories in computing and some in cybersecurity that educators and innovators can learn from. However, such efforts are likely to continue facing challenges when assessing learning and capturing broadly convincing evidence of transfer.

I. Perceptual and Coordinative Theory

In characterizing cognitive theories of transfer as "traditional," we do not mean to imply that cognitive theories of transfer are no longer being researched or extended. While we lack the space for full consideration, we alert readers to two specific strands of contemporary cognitive transfer research with direct implications and promise for cybersecurity education. The first is the *perceptual* transfer theory summarized in Day and Goldstone (2012). As summarized in Table 1, this research suggests that cybersecurity education should focus on the authenticity of the mental models that students are constructing in simulated learning environments rather than the authenticity of the actual environments. Given the massive investment in cyber ranges, this research suggests that designers should attend to what learners *perceive* in those environments, which may be very different than what learners are presented with.

The second specific contemporary contribution is the *coordinative* transfer theory summarized in Schwartz and Goldstone (2016). This theory builds on PFL to address the problem of *negative* transfer. This is where learners inappropriately "transfer in" prior knowledge to new situations. For example, a new cybersecurity graduate might inappropriately transfer adversarial thinking strategies learned in school into a very different initial job setting. Likewise, seasoned professionals might transfer (i.e., continue using) adversarial thinking strategies that were previously successful after those strategies become obsolete when the threat landscape evolves. With direct implications for cyber ranges and other simulations, Schwartz and Goldstone describe "overzealous transfer," where students mistakenly believe they were successful because of insufficient oversight. This reinforces negative transfer when such students fail to seek out corrective feedback. Schwartz and Goldstone summarize "productive failure" and other constructivist "inquiry-first" strategies. These strategies have been shown in rigorous experiments to help students recognize where their prior learning was and was not relevant in subsequent direct instruction.

While they are unlikely starting points, we suspect that perceptual and coordinative theories offer fundamentally new insights for designing and using cyber ranges and other sophisticated instructional technologies. These insights build on the more familiar cognitive theories but promise to address issues that are overlooked by those other theories. For example, Hickey and Kantor (in preparation) suggest that ideas from coordinative theory about negative transfer and failing to seek or provide corrective feedback may have profound implications for supporting the success of diverse and disadvantaged cybersecurity students. This is because associated power dynamics may downplay their relevant prior experience and ignore their requests for feedback.

VI. CONCLUSION

In summary, we are very enthusiastic about recent and continuing innovations in cybersecurity education, training, assessment, and certification. We agree with proponents of cyber ranges that they have already proven a worthwhile investment in this regard; we are enthusiastic about the potential of emerging technologies such as cyber ranges and digital twins, particularly when combined with augmented and virtual reality technologies. However, we also assume that these innovations will co-exist with conventional approaches and will not supplant them in the foreseeable future. We have argued that conventional and emerging approaches can all be improved by systematic and careful consideration of learning transfer for synergy between instruction, assessment, and testing.

This paper limited its consideration of transfer to relatively traditional "cognitive" theories of learning. We have shown how these theories might help innovators move beyond simplistic appeals to "active and authentic" learning and "alternative" assessment. We have also shown that each transfer theory raises crucial issues worthy of systematic investigation. These include the following, in this order:

- Differential theories of transfer that assume "learning" is whatever one's tests measure have negative implications that should be avoided (by not teaching to the test).
- Constructionist theories assume very general transfer of very general skills. They support popular innovations

like block-based programming and computational thinking. But many worry that this transfer is fleeting and overstated.

- A "general cognitive science" theory of transfer via analogical reasoning may be most relevant to many cybersecurity educators. This perspective is consistent with many prevailing approaches, sidesteps the enduring tensions between more specific approaches, and supports a massive research base.
- Cognitive-associationist theories assume specific transfer of very specific skills. They support artificially intelligent tutors, competency-based education, and other promising technologies and approaches. But some worry whether such learning transfers readily and widely.
- Constructivist theories assume specific transfer of general skills. They support helpful ideas like preparation for future learning and innovations like problem-based learning. But such learning is difficult to assess and may not transfer to high-stakes testing settings.
- New perceptual transfer theories suggest focusing on the authenticity of learners' schema rather than the authenticity of the features that define that actual learning and assessment environment.
- New coordinative transfer theories suggest using inquiry-first strategies to avoid negative transfer. They have unexplored implications for supporting conventional instruction and the needs of diverse and underrepresented learners.

In closing, we reiterate that we have taken a relatively objective stance toward these theories. This position reflects our enthusiasm for newer situative theories of learning and transfer. As elaborated in Hickey and Kantor (in review, in preparation), situative theories offer new solutions to some of the challenges raised in this paper and the challenge of better serving diverse learners. We hope that these papers together can together advance these important conversations.

REFERENCES

Abraham, S., & Shih, L. (2015). Instructional perspective: towards an integrative learning approach in cybersecurity education. *Information Security Education Journal*, *2*(2), 84-90. https://www.dline.info/isej/fulltext/v2n2/5.pdf

Alexander, R. C., Ma, L., Dou, Z. L., Cai, Z., & Huang, Y. (2023). Integrity, confidentiality, and equity: Using inquiry-based labs to help students understand AI and cybersecurity. *Journal of Cybersecurity Education, Research and Practice*, *2024*(1), 10. https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/10/

Amineh, R. J., & Asl, H. D. (2015). Review of constructivism and social constructivism. *Journal of Social Sciences, Literature, and Languages*, *1*(1), 9-16. https://studylib.net/doc/25304643/review-of-constructivism-and-social-constructivism

Ampel, B., Samtani, S., Zhu, H., Ullman, S., & Chen, H. (2020, November). Labeling hacker exploits for proactive cyber threat intelligence: a deep transfer learning approach. In *2020 IEEE international conference on intelligence and security informatics (ISI)* (pp. 1-6). IEEE. https://ieeexplore.ieee.org/abstract/document/9280548

Anderson, J. R. (1982) Acquisition of cognitive skill. *Psychological Review 89* (4), 369-406. https://doi.org/10.1037/0033-295X.89.4.369

Association for Computing Machinery (2017). *Cybersecurity curricula 2017.https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf*

Austin, G. (Ed.) (2021). *Cyber security education: Principles and policies.* Routledge. ISBN 9780367421915.

Beauchamp, C., & Matusovich, H. M. (2023). A Mixed-method study exploring cyber ranges and educator motivation. *Journal of Cybersecurity Education, Research and Practice*, *2023*(2), 7. DOI: 10.32727/8.2023.21, https://digitalcommons.kennesaw.edu/jcerp/vol2023/iss2/7/

Bécue, A., Fourastier, Y., Praça, I., Savarit, A., Baron, C., Gradussofs, B., ... & Thomas, C. (2018, June). CyberFactory# 1—Securing the industry 4.0 with cyber-ranges and digital twins. In *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)* (pp. 1-4). IEEE. https://ieeexplore.ieee.org/abstract/document/8402377

Bernard, L., Raina, S., Taylor, B., & Kaza, S. (2021, May). Minimizing cognitive load in cyber learning materials–An eye tracking study. In *ACM Symposium on Eye Tracking Research and Applications* (pp. 1-6). https://doi.org/10.1145/3448018.3458617

Black, P., & Wiliam, D. (1998). Assessment and classroom learning. *Assessment in Education: Principles, Policy & Practice, 5*(1), 7–74. https://doi.org/10.1080/0969595980050102

Bier, N., Lovett, M., & Seacord, R. (2011). An online learning approach to information systems security education. In *Proceedings of the 15th Colloquium for Information Systems Security Education* (pp. 56-62). ISBN 1-933510-96-X.

Bill and Melinda Gates Foundation (2011). *Supporting students: Investing in innovation and quality.* [Monograph]. https://docs.gatesfoundation.org/documents/supporting-students.pdf.

Böhm, F., Dietz, M., Preindl, T., & Pernul, G. (2021). Augmented reality and the digital twin: State-of-the-art and perspectives for cybersecurity. *Journal of Cybersecurity and Privacy*, *1* (3), 519-538. https://doi.org/10.3390/jcp1030026

Bowen, D., Jaurez, J., Jones, N., Reid, W., & Simpson, C. (2022). Cybersecurity educational resources for K-12. *Journal of Cybersecurity Education, Research and Practice*, *2022*(1), 6. : https://digitalcommons.kennesaw.edu/jcerp/vol2022/iss1/6

Bransford, J. D., & Schwartz, D. L. (1999). Rethinking transfer: A simple proposal with multiple implications. *Review of Research in Education, 24*, 61-100. https://doi.org/10.3102/0091732X024001061

Burrows, A. C., Borowczak, M., & Mugayitoglu, B. (2022). Computer science beyond coding: Partnering to create teacher cybersecurity microcredentials. *Education Sciences*, *12*(1), 4. https://doi.org/10.3390/educsci12010004

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*, *75*, 24-35. https://doi.org/10.1016/j.cose.2018.01.015

Caelli, W. J. (2020). History and philosophy of cyber security education. In G. Austin (Ed.) *Cyber security education: Principles and policies* (pp. 8-28). Routledge. ISBN: 9780367822576

CBT Nuggets (2024, January 8). *The need for cybersecurity training has never been greater* [Website]. https://www.cbtnuggets.com/it-training/cyber-security.

Chan Zuckerberg Initiative (2017; October 30). *Expanding access to personalized learning opportunities with the College Board.* [Blogpost]. https://chanzuckerberg.com/newsroom/expanding-access-to-personalized-learning-oppotunities-with-the-college-board/

Chowdhury, N., & Gkioulos, V. (2023). A personalized learning theory-based cyber-security training exercise. *International Journal of Information*

Security, 22, 1531-1546. https://doi.org/10.1007/s10207-023-00704-z

Cognition and Technology Group at Vanderbilt. (1990). Anchored instruction and its relationship to situated cognition. *Educational Researcher*, *19*(6), 2-10. https://www.jstor.org/stable/44427992

Comprehensive National Cybersecurity Initiative. (2023, September, 10). In *Wikipedia.* *https://en.wikipedia.org/wiki/Comprehensive_National_Cybersecurity_Initiative*

Conklin, W. A., Whjite, G., Cothren, C., Davis, R., & Williams, D. (2022). *Principles of computer security: CompTIA Security+ and beyond* (Sixth Edition). McGraw Hill. ISBN13: 9781260474312.

Corporation for Public Broadcasting (2022, August 12). *Cybersecurity lab* [Website] https://www.pbs.org/wgbh/nova/labs/lab/cyber/

Cusak, A. (2023). Case study: The impact of emerging technologies on cybersecurity education and orkforces. *Journal of Cybersecurity Education, Research and Practice*, *2023*(1), 3. https://digitalcommons.kennesaw.edu/jcerp/vol2023/iss1/3/

Cybersecurity Skills Journal (2024, January 8). *About CSJ* [Journal homepage]. https://www.nationalcyberwatch.org/cybersecurity-skills-journal-practice-and-research/

Daimi, K., & Francia, G. (Eds.). (2020). *Innovations in cybersecurity education*. Springer. ISBN: 978-3-030-50243-0

Dark, M. (2014). Advancing cybersecurity education. *IEEE Security & Privacy*, *12*(6), 79-83. https://ieeexplore.ieee.org/abstract/document/7006436

Dark, M. (2015). Thinking about cybersecurity. *IEEE Security & Privacy*, *13*(1), 61-65. https://ieeexplore.ieee.org/abstract/document/7031840

Day, S. B., & Goldstone, R. L. (2012). The import of knowledge export: Connecting findings and theories of transfer of learning. *Educational Psychologist*, *47*(3), 153-176. https://doi.org/10.1080/00461520.2012.696438

Deng, Y., Lu, D., Chung, C. J., Huang, D., & Zeng, Z. (2018, October). Personalized learning in a virtual hands-on lab platform for computer science education. In *2018 IEEE Frontiers in Education Conference (FIE)* (pp. 1-8). IEEE. https://ieeexplore.ieee.org/abstract/document/8659291

Detterman, D. K., & Sternberg, R. J. (1993). *Transfer on trial: Intelligence, cognition, and instruction*. Ablex Publishing. ***ISBN-10: 0893918261***

Dupuis, M. J. (2017). Cyber security for everyone: An introductory course for non-technical majors. *Journal of Cybersecurity Education, Research and Practice*, *1.* 3. https://digitalcommons.kennesaw.edu/jcerp/vol2017/iss1/3

Engle, R. A. (2012). The resurgence of research into transfer: An introduction to the final articles of the transfer strand. *Journal of the Learning Sciences*, *21*(3), 347-352. https://doi.org/10.1080/10508406.2012.707994

Engle, R. A., Lam, D. P., Meyer, X. S., & Nix, S. E. (2012). How does expansive framing promote transfer? Several proposed explanations and a research agenda for investigating them. *Educational Psychologist*, *47*(3), 215-231. https://doi.org/10.1080/00461520.2012.695678

Frederiksen, J. R., & Collins, A. (1989). A systems approach to educational testing. *Educational Researcher*, *18*(9), 27-32. https://www.jstor.org/stable/1176716

Frezzo, D. C., Behrens, J. T., & Mislevy, R. J. (2010). Design patterns for learning and assessment: Facilitating the introduction of a complex simulation-based learning environment into a community of instructors. *Journal of Science Education and Technology*, *19*(2), 105-114. https://link.springer.com/article/10.1007/s10956-009-9192-0

Gagné RM. (1985). *The conditions of learning and theory of instruction*. Holt, Rinehart and Winston; New York. *ISBN-10. 9780030636882*

Gallagher, P. S. (2016). Assessing performance in an innovative cybersecurity pilot course. *Interservice/industry training, simulation, and education conference* https://adlnet.gov/assets/uploads/Assessing-Performance-in-an-Innovative-Cybersecurity

Giboney, J. S., McDonald, J. K., Balzotti, J., Hansen, D. L., Winters, D. M., & Bonsignore, E. (2021). Increasing cybersecurity career interest through playable case studies. *TechTrends*, *65*(4), 496-510. https://doi.org/10.1007/s11528-021-00585-w

Glaser, R. (1984). Education and thinking: The role of knowledge. *American Psychologist*, *39*(2), 93-104. https://doi.org/10.1037/0003-066X.39.2.93

Goldstone, R. L., & Day, S. B. (2012). New conceptualizations of transfer of learning [Special Issue] *Educational Psychologist*, *47*(3). https://doi.org/10.1080/00461520.2012.695710

González-Torres, A., Hernández-Campos, M., González-Gómez, J., Byrd, V. L., & Parsons, P. (2020). Information visualization as a method for cybersecurity education. In K. Daimi & G. Francia (Eds.), *Innovations in Cybersecurity Education* (pp. 55-70). Springer. https://link.springer.com/chapter/10.1007/978-3-030-50244-7_4

Greeno, J. G. (1998). The situativity of knowing, learning, and research. *American Psychologist*, *53*(1), 5-30. https://doi.org/10.1037/0003-066X.53.1.5

Greeno, J. G., Collins, A., & Resnick, L. B. (1996). Cognition and learning. In D. C. Berliner & R. C. Calfee (Eds.), *Handbook of educational psychology* (pp. 15–46). Simon & Schuster Macmillan. https://doi.org/10.4324/9780203053874

Grover, S., Basu, S., Bienkowski, M., Eagle, M., Diana, N., & Stamper, J. (2017). A framework for using hypothesis-driven approaches to support data-driven learning analytics in measuring computational thinking in block-based programming environments. *ACM Transactions on Computing Education (TOCE)*, *17*(3), 1-25. https://doi.org/10.1145/3105910

Gupta, A., & Wolf, J. R. (2018). An examination of cybersecurity knowledge transfer: Teaching, research, and website security at US colleges and universities. *Journal of Cybersecurity Education, Research and Practice*, *2*, 4. https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss2/4/

Guzdial, M. (2010). Does contextualized computing education help?. *ACM Inroads*, *1*(4), 4-6. https://doi.org/10.1145/1869746.1869747

Haertel, E. H. (1999). Performance assessment and education reform. *Phi Delta Kappan*, *80*(9), 662-666. https://www.jstor.org/stable/20439533.

Hamman, S. T., & Hopkinson, K. M. (2016, October). Teaching adversarial thinking for cybersecurity. *Journal of the Colloquium for Information Systems Security Education*, *4* (1), 1-19. https://cisse.info/journal/index.php/cisse/article/view/56

Hickey, D. T., Chartrand, G. T., & Andrews, C. D. (2020a). Expansive framing as pragmatic theory for online and hybrid instructional design. *Educational Technology Research and Development*, *68*, 751-782. https://doi.org/10.1007/s11423-020-09759-4

Hickey, D. T., Duncan, J., Gaylord, C., Hitchcock, C., Itow, R., & Stephens, S. (2020b). gPortfolios: A pragmatic approach to online asynchronous assignments. *Information and Learning Sciences, 121* (5/6), 273-283. https://doi.org/10.1108/ILS-04-2020-0094

Hickey, D., & Harris, T. (2021). Reimagining online grading, assessment, and testing using situated cognition. *Distance Education*, *42*(2), 290-309. https://doi.org/10.1080/01587919.2021.1911627

Hickey, D. T., Ingram-Goble, A. A., & Jameson, E. M. (2009). Designing assessments and assessing designs in virtual educational environments. *Journal of Science Education and Technology*, *18*, 187-208. https://doi.org/10.1007/s10956-008-9143-1

Hickey, D. T., & Kantor, R, J. (in review). Transforming cybersecurity instruction, assessment, and testing with personal authenticity and situative transfer theory. Accepted for review, *Computer Science Education,* February, 2024

Hickey, D. T., & Kantor, R. J. (in preparation). Transfer of learning and diversity, equity, and inclusion in cybersecurity education and training.

Hickey, D. T., Kindfield, A. C., Horwitz, P., & Christie, M. T. (2003). Integrating curriculum, instruction, assessment, and evaluation in a technology-supported genetics learning environment. *American Educational Research Journal*, *40*(2), 495-538. https://doi.org/10.3102/00028312040002

Hickey, D. T., Luo, Q. M., & Lam, C. (in press). A stridently situative perspective on inclusive engagement and assessment. Accepted for publication in G. A. D. Liem, J. Fredricks, & Z. Y. Wong (Eds.), *Research on sociocultural influences on motivation and learning.* Information Age Publishing.

Hickey, D., & Pellegrino, J. W. (2005). Theory, level, and function. Three dimensions of transfer for understanding student assessment. In J. Mestre (Ed.) *Transfer of learning from a modern multidisciplinary perspective* (pp. 251-293). Information Age Publishing. ISBN 10: 1593111649

Hickey, D., & Rehak, A. (2013). Wikifolios and participatory assessment for engagement, understanding, and achievement in online courses. *Journal of Educational Multimedia and Hypermedia*, *22*(4), 407-441. https://www.learntechlib.org/p/41508/

Hickey, D. T., Wolfe, E. W., & Kindfield, A. C. (2000). Assessing learning in a technology-supported genetics environment: Evidential and systemic validity issues. *Educational Assessment*, *6*(3), 155-196. https://doi.org/10.1207/S15326977EA0603_1

Hickey, D. T., & Zuiker, S. J. (2012). Multilevel assessment for discourse, understanding, and achievement. *Journal of the Learning Sciences*, *21*(4), 522-582. https://doi.org/10.1080/10508406.2011.652320

Hmelo-Silver, C. E. (2004). Problem-based learning: What and how do students learn? *Educational Psychology Review*, *16*(3), 235-266. https://link.springer.com/article/10.1023/B:EDPR.0000034022.16470.f3

Ibrahim, A., & Ford, V. (2021). Observations, evaluations, and recommendations for DETERLab from an educational perspective. *Journal of Cybersecurity Education, Research and Practice*, *1*, 4. https://digitalcommons.kennesaw.edu/jcerp/vol2021/iss1/4/

Kafai, Y. B., & Proctor, C. (2022). A revaluation of computational thinking in K–12 education: Moving toward computational literacies. *Educational Researcher*, *51*(2), 146-151. https://doi.org/10.3102/0013189X211057904

Kafai, Y., Resnick, M. (1996). *Constructionism in practice: Designing, thinking, and learning in a digital world*. Routledge. ISBN 9780805819847

Karjalainen, M., & Kokkonen, T. (2020, September). Comprehensive cyber arena; the next generation cyber range. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 11-16). IEEE. https://ieeexplore.ieee.org/abstract/document/9229857

Klein, S., Benjamin, R., Shavelson, R., & Bolus, R. (2007). The Collegiate Learning Assessment: Facts and fantasies. *Evaluation Review. 31*(5), 415-439; https://doi.org/10.1177/0193841X07303318

Koedinger, K. R., Corbett, A. T., & Perfetti, C. (2012). The Knowledge-Learning-Instruction framework: Bridging the science-practice chasm to enhance robust student learning. *Cognitive Science*, *36*(5), 757-798. https://doi.org/10.1111/j.1551-6709.2012.01245.x

Konak, A. (2018). Experiential learning builds cybersecurity self-efficacy in K-12 students. *Journal of Cybersecurity Education, Research and Practice*, *1,* 6. https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss1/6/

Konak, A., & Bartolacci, M. R. (2016). Using a virtual computing laboratory to foster collaborative learning for information security and information technology education. *Journal of Cybersecurity Education, Research and Practice*, *1,* 2. https://digitalcommons.kennesaw.edu/jcerp/vol2016/iss1/2/

Laato, S., Farooq, A., Tenhunen, H., Pitkamaki, T., Hakkala, A., & Airola, A. (2020, July). A.I. in cybersecurity education: A systematic literature review of studies on cybersecurity MOOCs. In *2020 IEEE 20th International Conference on Advanced Learning Technologies* (pp. 6-10). https://ieeexplore.ieee.org/abstract/document/9156050

Lamon, M., Secules, T., Petrosino, A. J., Hackett, R., Bransford, J. D., & Goldman, S. R. (2013). Schools for thought: Overview of the project and lessons learned from one of the sites. *Innovations in Learning*, 243-288. https://scholarlycommons.pacific.edu/ed-facbooks/29/

Lesko, C. J. (2019). A design case: Assessing the functional needs for a multi-faceted cybersecurity learning space. *Journal of Cybersecurity Education, Research and Practice*, *1*, 6. https://digitalcommons.kennesaw.edu/jcerp/vol2019/iss1/6/

Lewis, J. A. (2019, January 20). *The cybersecurity workforce gap.* [Report]. Center for Strategic and International Studies. https://www.csis.org/analysis/cybersecurity-workforce-gap

Lobato, J. (2006). Alternative perspectives on the transfer of learning: History, issues, and challenges for future research. *The Journal of the Learning Sciences*, *15*(4), 431-449. https://www.jstor.org/stable/25473530

Lumina Foundation (2024, January 8). *Competency-based Education/* [Website]. https://www.luminafoundation.org/our-work/competency-based-learning/

Marquardson, J., & Elnoshokaty, A. (2020). Skills, certifications, or degrees: What companies demand for entry-level cybersecurity jobs. *Information Systems Education Journal*, *18*(1), 22-28. https://eric.ed.gov/?id=EJ1246234

Margulieux, L. E., Catrambone, R., & Guzdial, M. (2016). Employing subgoals in computer programming education. *Computer Science Education*, *26*(1), 44-67. https://doi.org/10.1080/08993408.2016.1144429

Margulieux, L., Denny, P., Cunningham, K., Deutsch, M., & Shapiro, B. R. (2021, August). When wrong is right: The instructional power of multiple conceptions. In *Proceedings of the 17th ACM Conference on International Computing Education Research* (pp. 184-197). https://doi.org/10.1145/3446871.3469750.

Mayer, R. E. (Ed.). (2005). *The Cambridge handbook of multimedia learning*. Cambridge University Press. ISBN 978-1-107-03520-1

Mayer, R. E., & Wittrock, M. C. (1996). Problem-solving transfer. In D. C. Berliner & R. C. Calfee (Eds.), *Handbook of educational psychology* (pp. 47–62). Macmillan. https://doi.org/10.4324/9780203053874

Messick, S. (1994). The interplay of evidence and consequences in the validation of performance assessments. *Educational Researcher*, *23*(2), 13-23. https://doi.org/10.3102/0013189X023002013

Mestre, J. P. (Ed.). (2006). *Transfer of learning from a modern multidisciplinary perspective*. Information Age Publishing. ISBN 1-59311 164 - 9

Mishra, S., Raj, R. K., Tymann, P., Fagan, J., & Miller, S. (2017, October). CyberCSP: Integrating cybersecurity into the computer science principles course. In *2017 IEEE Frontiers in Education Conference (FIE)* (pp. 1-5). https://ieeexplore.ieee.org/abstract/document/8190711

Mislevy, R. J. (1996). Test theory reconceived. *Journal of Educational Measurement* (Vol. 33, Issue 4, pp. 379–416). https://doi.org/10.1111/j.1745-3984.1996.tb00498.x

Mountrouidou, X., Li, X., & Burke, Q. (2018, July). Cybersecurity in liberal arts general education curriculum. In *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer*

Science Education (pp. 182-187). https://doi.org/10.1145/3197091.3197110

Murphy, J., Sihler, E., Ebben, M., & Wilson, G. (2014). Building a virtual cybersecurity collaborative learning laboratory (VCCLL). In *2014 World Congress in Computer Science, Conference Proceedings: Computer Engineering and Applied Computing*. https://digitalcommons.usm.maine.edu/cgi/viewcontent.cgi?article=1020&context=philosophy-faculty

National Academies of Sciences, Engineering, and Medicine. (2018). *How people learn II; Learners, contexts, and cultures*. National Academies Press. https://doi.org/10.17226/24783

National Academies of Sciences, Engineering, and Mathematics (2021). *Cultivating interest and competencies in computing: Authentic experiences and design factors.* National Academy Press. https://doi.org/10.17226/25912

National Academy of Sciences, Engineering, and Medicine (2024, January 6). *Guidelines for the review of products of the National Academies of Sciences, Engineering, and Medicine.* [Website]. https://www.nationalacademies.org/about/institutional-policies-and-procedures/guidelines-for-the-review-of-reports

National Institute for Cybersecurity Education (2018). *The cyber range: A guide.* Author. https://www.nist.gov/document/cyber-range

National Institute for Cybersecurity Education (2020). *NICE workforce framework for cybersecurity.* Author https://niccs.cisa.gov/workforce-development/nice-framework

National Research Council (1999). *How people learn*: *Brain, mind, & experience.* National Academies Press. DOI: https://doi.org/10.17226/9853

National Research Council. (2001). *Knowing what students know: The science and design of educational assessment*. National Academies Press. https://doi.org/10.17226/10019

National Research Council. (2013). *Professionalizing the nation's cybersecurity workforce?: Criteria for decision-making*. National Academies Press. https://doi.org/10.17226/18446

Noponen, S., Parssinen, J., & Salonen, J. (2022). Cybersecurity of cyber ranges: Threats and mitigations. *International Journal for Information Security Research*, *12*(1), 1032-1040. https://doi.org/10.20533/ijisr.2042.4639.2022.0117

Olson, D. R., & Bruner, J. S. (1996). Folk psychology and folk pedagogy. In D. R. Olson & N. Torrance (Eds) *The handbook of education and human development. New models of learning, Teaching and schooling* (pp. 9-27). Blackwell https://doi.org/10.1111/b.9780631211860.1998.00003.x

Padmos, A. (2018, August). Against mindset. In *Proceedings of the New Security Paradigms Workshop* (pp. 12-27). https://dl.acm.org/doi/10.1145/3285002.3285004

Papano, L. (2017, April 4). Learning to think like a computer. *The New York Times.* https://www.nytimes.com/2017/04/04/education/edlife/teaching-students-computer-code.html

Papert, S. A. (1980). *Mindstorms*. Basic Books. https://doi.org/10.1007/978-3-0348-5357-6

Payne, B. R., Abegaz, T., & Antonia, K. (2016). Planning and implementing a successful nsa-nsf GenCyber summer cyber academy. *Journal of Cybersecurity Education, Research and Practice*, *2,* 3. https://digitalcommons.kennesaw.edu/jcerp/vol2016/iss2/3

Payne, B. K., Mayes, L., Paredes, T., Smith, E., Wu, H., & Xin, C. (2021). Applying high-impact practices in an interdisciplinary cybersecurity program. *Journal of Cybersecurity Education, Research and Practice*, *2,* 4. https://digitalcommons.kennesaw.edu/jcerp/vol2020/iss2/4

Pellegrino, J. W. (2018). Assessment of and for learning. In F. Fischer, C. Hmelo-Silver, S. R. Goldman, & P, Reimann (Eds), *International handbook of the learning sciences* (pp. 410-421). Routledge. ISBN 9781138670594.

Pellegrino, J. W., DiBello, L. V., & Goldman, S. R. (2016). A framework for conceptualizing and evaluating the validity of instructionally relevant assessments. *Educational Psychologist*, *51*(1), 59-81. https://doi.org/10.1080/00461520.2016.1145550

Pellegrino, J. W., & Glaser, R. (1982). Analyzing aptitudes for learning: Inductive reasoning. In R. Glaser (Ed.), Advances in instructional psychology (Vol. 2, pp. 269-345). Erlbaum. https://doi.org/10.4324/9781315864341

Piaget, J. (1954). *The construction of reality by a child.* Translated by Margaret Cook. Basic Books. https://doi.org/10.1037/11168-000

Piety, P. J., Bonsignore, E. M., Hansen, D. L., & Hickey, D. T. (2019-2024). *Collaboration in the Future of Work: Developing playable case studies to improve STEM Career pathways.* Project funded by the US National Science Foundation's Improving Undergraduate STEM Education Program IUSE # 1915498. https://careersinplay.umd.edu/

Reed, S. K. (2020). Searching for the big pictures. *Perspectives on Psychological Science*, *15*(3), 817-830. https://doi.org/10.1177/1745691619896255.

Robins, A. V., Margulieux, L. E., & Morrison, B. B. (2019). Cognitive sciences for computing education. In S. A. Fincher & A. V. Robins (Eds.) *The Cambridge handbook of computing education research* (pp. 231-275). Cambridge University Press. https://doi.org/10.1017/9781108654555

Sanders, K., Boustedt, J., Eckerdal, A., McCartney, R., & Zander, C. (2017, August). Folk pedagogy: Nobody doesn't like active learning. In *Proceedings of the 2017 ACM Conference on International Computing Education Research* (pp. 145-154). https://doi.org/10.1145/3105726.3106192

Schwartz, D. L., & Goldstone, R. (2016). Learning as coordination: Cognitive psychology and education. In L. Corno & E. M. Anderman (Eds.), *Handbook of educational psychology, 3rd ed.* (pp. 61–75). Routledge. https://doi.org/10.4324/9781315688244

Seda, P., Vykopal, J., Švábenský, V., & Čeleda, P. (2021, October). Reinforcing cybersecurity hands-on training with adaptive learning. In *2021 IEEE Frontiers in Education Conference (FIE)* (pp. 1-9). https://doi.org/10.1109/FIE49875.2021.9637252

Shepard, L. A. (2000). The role of assessment in a learning culture. *Educational Researcher*, *29*(7), 4-14. https://doi.org/10.3102/0013189X029007004

Shivapurkar, M., Bhatia, S., & Ahmed, I. (2020, July). Problem-based learning for cybersecurity education. In *Journal of The Colloquium for Information Systems Security Education* (Vol. 7, No. 1, pp. 6-16). https://cisse.info/journal/index.php/cisse/article/view/108

Singley, M. K., & Anderson, J. R. (1989). *The transfer of cognitive skill*. Harvard University Press. ISBN-10: 0674903404

Skinner, B. F. (1958). Teaching machines. *Science, 128* (3330), 137-158. https://doi.org/10.1126/science.128.3330.969

Snow, E., Rutstein, D., Basu, S., Bienkowski, M., & Everson, H. T. (2019). Leveraging evidence-centered design to develop assessments of computational thinking practices. *International Journal of Testing*, *19*(2), 103-127. https://doi.org/10.1080/15305058.2018.1543311

Stecher, B. M., & Klein, S. P. (1997). The cost of science performance assessments in large-scale testing programs. *Educational Evaluation and Policy Analysis*, *19*(1), 1-14. https://doi.org/10.2307/1164516

Sternberg, R. J. (1990). *Metaphors of mind: Conceptions of the nature of intelligence*. Cambridge University Press. ISBN 0-521-35579-6

Thompson, J. D., Herman, G. L., Scheponik, T., Oliva, L., Sherman, A., Golaszewski, E., ... & Patsourakos, K. (2018). Student misconceptions

about cybersecurity concepts: Analysis of think-aloud interviews. *Journal of Cybersecurity Education, Research and Practice*, *1,* 5. https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss1/5/

Tobey, D. H. (2018) Raising the BAR of cybersecurity capability maturity: *Cybersecurity Skills Journal: Practice and Research, 20,* 6-14 https://www.nationalcyberwatch.org/wp-content/uploads/2018/08/2018_CSJ_3CS_Special_Issue_FINAL.pdf

Tobey, D. H., Gandhi, R. A., Watkins, A. B., & O'Brien, C. W. (2018). Competency is not a three-letter word. *Cybersecurity Skills Journal: Practice and Research*, *20*, 32-38. https://www.researchgate.net/profile/David-Tobey-2/publication/328103062

TrainingCamp (2024, Janaury 6) (ISC) *Official CISSP certification boot camp.* [Website]. https://trainingcamp.com/

Tran, B., Benson, K. C., & Jonassen, L. (2023). Integrating certifications into the cybersecurity college curriculum: The efficacy of education with certifications to increase the cybersecurity workforce. *Journal of Cybersecurity Education, Research and Practice*, *2*, 2. https://digitalcommons.kennesaw.edu/jcerp/vol2023/iss2/2

Vykopal, J., Seda, P., Švábenský, V., & Čeleda, P. (2022). Smart environment for adaptive learning of cybersecurity skills. *IEEE Transactions on Learning Technologies*. **DOI:** 10.1109/TLT.2022.3216345

White House (2010). *The comprehensive national cybersecurity initiative.* https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative

Whitman, M. E., & Mattord, H. J. (2016). Threats to information protection-industry and academic perspectives: an annotated bibliography. *Journal of Cybersecurity Education, Research and Practice*, 2, 4. https://digitalcommons.kennesaw.edu/jcerp/vol2016/iss2/4/

Wiggins, G. (1998). *Educative assessment: Designing assessments to inform and improve student performance*. Jossey-Bass Publishers. **ISBN:** ISBN-0-7879-0848-7.

Williams, B. A. (2022). Editorial: Introducing *Principia* and contemporary classical education. *Principia: A Journal of Classical Education, 1* (1). 1-14. https://doi.org/10.5840/principia202211/21

Wolf, D., Bixby, J., Glenn, J., & Gardner, H. (1991). To use their minds well: Investigating new forms of student assessment. *Review of Research in Education*, *17*(1), 31–74. https://www.jstor.org/stable/1167329

Workman, M. D. (2021). An exploratory study of mode efficacy in cybersecurity training. *Journal of Cybersecurity Education, Research and Practice*, *1,* 2. https://digitalcommons.kennesaw.edu/jcerp/vol2021/iss1/2/

Yadav, A., Krist, C., Good, J., & Caeli, E. N. (2018). Computational thinking in elementary classrooms: Measuring teacher understanding of computational ideas for teaching science. *Computer Science Education*, *28*(4), 371-400. https://doi.org/10.1080/08993408.2018.1560550

Yett, B., Hutchins, N., Stein, G., Zare, H., Snyder, C., Biswas, G., ... & Lédeczi, Á. (2020, February). A hands-on cybersecurity curriculum using a robotics platform. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (pp. 1040-1046). https://doi.org/10.1145/3328778.3366878

Zhang, L., & Nouri, J. (2019). A systematic review of learning computational thinking through Scratch in K-9. *Computers & Education*, *141*, 103607. https://doi.org/10.1016/j.compedu.2019.103607

Appendix 1

Implications of Cognitive Transfer Theories for Cybersecurity Education

Learning & Transfer Theory	What Are Learners Doing?	How Does Learning Transfer?	How Should We Design Instruction?	What Should We Assess and How?	Cybersecurity Examples
Differential Theory	Whatever is needed to pass a test.	Very general transfer of very general skills.	Whatever is needed to boost test scores without cheating	General and specific skills using psychometrics.	Some cybersecurity education and most certification tests.
Constructionism	Constructing very general schema making sense of the world.	Very general transfer of very general thinking skills ("formal discipline").	Use "open-ended" problems that require very general skills.	Avoid specific assessments and tests; assess computational thinking.	*Scratch*, block-based programming, computational thinking.
General Cognitive Science	Metacognitively managing the acquisition of specific and general skills.	Analogies (abstract mental models) created in the learning environments are used to solve new problems.	Start with basic skills and build up to complex authentic problems; avoid cognitive load.	Ability to solve specific and general new problems; avoid "traditional" tests.	"Active" and "authentic" learning, cyber ranges, digital twins. Mayer's multimedia learning.
Cognitive-Associationism	Acquiring specific associations directly from the environment.	Specific transfer of very specific skills.	Directly present carefully sequenced associations; avoid cognitive load.	Assess mastery of specific associations using conventional tests.	Cognitive tutors, adaptive learning technologies, competency-based ed, many MOOCs.
Constructivism	Constructing general schema to make sense of domains.	Specific transfer of general skills.	Investigate complex authentic problems from the start.	Ability to solve new problems; avoid traditional tests.	Discovery and inquiry learning, and some experiential and project-based learning.
Social Constructivism	Collaboratively constructing general schema to make sense of domains.	Specific transfer of general skills in collaboration.	Collaboratively investigate complex authentic problems from the start.	Preparation for future learning, avoid all isolated "static" tests.	Collaborative experiential and project-based learning, problem-based learning, anchored instruction.
Perceptual Transfer	Perceiving schema while making sense of the world.	Use general schema to solve new problems perceptually.	Ensure students construct authentic schema.	Ability to solve new problems, avoid traditional tests.	Authentic perceptions rather than authentic contexts.
Coordinative Transfer	Perceiving schema while making sense of the world	Sometimes transfer is overzealous and negative	Productive failing and inquiry before expository instruction	Preparation for future learning, avoid static tests.	Inquiry first and productive failure strategies.