Using Complexity Theory to Identify K-12+ Pedagogical Misalignment With a Security Mindset

Holly Hanna
Wilkes University
Wilkes-Barre, USA
holly.hanna@wilkes.edu

Jane Blanken-Webb
Wilkes University
Wilkes-Barre, USA
jane.blankenwebb@wilkes.edu

Abstract—The current state of growing connectivity in society calls for a security mindset for K-12 and post-secondary (K-12+) populations. A security mindset offers an important approach to support security and can usefully be understood through the lens of complexity theory. Complexity theory also provides a helpful lens for identifying limitations inherent within some common pedagogical frameworks and practices in K-12+ education systems that may pose challenges for the cultivation of a security mindset. Hence, this paper brings awareness to examples of some of the most prominent pedagogical frameworks and practices that stand in potential misalignment with a security mindset when they are implemented in an imposing, monolithic manner. These include: rigid, prescriptive curricula; binary thinking, compliance, and standardized assessments; and disciplinary constraints. By identifying ways that common pedagogical practices stand to potentially undermine the cultivation of a security mindset, this paper contributes to clearing the way forward for K-12+ educational systems to design for emergence in support of building a more secure society.

Keywords—security mindset, complexity, K-12+ education, cybersecurity

I. Introduction

With increasing socio-technical interdependence and growing global connectivity, cyber experts recognize the need for end users to actively contribute to cybersecurity measures [1], [2]. While end users are not expected to possess the technical knowledge of cyber experts [3], it is important they develop a security mindset [1]. Such a security mindset can be cultivated within general populations through supporting end users to think beyond isolated security practices in order to negotiate increasingly complex, interwoven networks that are always in flux [1].

In this paper, we identify pedagogical frameworks and practices within K-12+ education systems that pose challenges for the holistic cultivation of a security mindset. From a systemic level, it is important for schools to reframe the way they view cybersecurity to ensure they implement robust routines that foster a security mindset and not simply content and isolated practices that stand alone. Strictly speaking, thinking in this manner, involves a metacognitive leap from applying concrete skills and applications within finite, traditional systems, to conceptualizing and responding to emergent structures within complex systems (i.e. systems within systems). We propose that there is an inherent challenge to teaching this way of thinking, as doing so requires pushing beyond the typical structures of educational practice itself. Hence, the metacognitive leap entailed in a security mindset pushes away from aspects of traditional systems of schooling and moves toward complex thinking. Thus, we urge educators to step beyond an overreliance on traditional frameworks and practices that have the potential to leave end users ill-equipped to adapt to today's highly complex, interdependent socio-technical systems.

II. Increased Interdependence and Emerging Complexity

Interdependencies between humans, devices and their environments are rapidly deepening [2], [4], [5], as “Everything is becoming one complex hyper-connected system in which, even if things don’t interoperate, they’re on the same network and affect each other” [6, p. 26]. As society becomes more connected and reliant on this network, cyber threats become more prevalent and sophisticated [3]. Additionally, the ever-changing nature of technology creates increasing complexity [6], requiring responses beyond the conventional linear, planned steps that were appropriate in the past yet fall short within the current “Age of Complexity” [4], [5], [7, p. 31]. Once predictable, clear cause and effect responses now beg for more crucial adaptive, bottom-up approaches [4], [5]. Instead of relying on past routines as the model for future responses, the dynamic nature of the hyperconnected network and society as a whole require a flexible mindset, strategically ebbing and flowing with the current of unpredictability. The reality we live in is rapidly changing and we need to adapt accordingly [5].

III. Security Mindset

Embedded in mounting calls to build societal resilience against escalating cyber attacks [8], [9], is a recognition that end users need to take reasonable responsibility for “themselves and their network of users” rather than placing sole responsibility on the shoulders of cyber experts [1, p. 3], [2], [3]. In their 2020 report, the Cyberspace Solarium Commission (CSC) proposes: “The U.S. government should promote digital literacy, civics education, and public awareness to build societal resilience to foreign malign cyber-enabled information operations" [9, p. 98]. The report further encourages improved digital citizenship through a digital literacy curriculum for K-12 and beyond.

Experts acknowledge that "the end user can be a critical backdoor into the network" [10, p. 3]. However, others affirm that the end user should be viewed as a solution rather than a problem [2, 3]. When end users are seen as active, positive participants rather than compliant, "rule followers," they are more likely to develop the skills needed to adapt to evolving creative attacks [2, p. 174]. Consciousness is conjured by creativity [11] and this underscores the viability of shifting control and innovation from a central group of cyber experts to society as a whole to at least some extent. Furthermore, "Creating systems that would centrally protect end-users would also undermine their role in creating and using the internet in powerful ways" [2, p. 2]. Additionally, experts suggest attention not only be placed on the technical aspects of cybersecurity but also on the social and human behaviors that lead to both security success and errors [2], [12].

With increasing information and technological advances projected to reach cognitive levels beyond human limits [13], developing a security mindset is crucial. Per Crum et al., "mindset" is defined as "a mental frame or lens that selectively organizes and encodes information, thereby orienting an individual toward a unique way of understanding an experience and guiding one toward corresponding actions and responses" [14, p. 717]. A security mindset has the potential to support end users in thinking beyond an extensive list of security practices to sculpt security behaviors into enduring habits in which end users continually adapt to new threats and take appropriate measures [1], [2], [3], [15]. A security mindset creates a more sustainable approach to security rather than the monolithic reliance on current practices that are predicted to transform dramatically as quantum computing further develops [16].

IV. Complexity Theory and Cybersecurity

Complexity theory has become increasingly significant due to growing, global connectedness and evolving societal issues referred to as "wicked problems," [4], [5] appropriately named not because they are evil but because they have no definitive problem or solution [6]. Global climate change, terrorism [5], and the hyperconnected network [6] are a few examples. Wicked problems are constantly affected by changing variables; therefore, "Attempting to address wicked problems using traditional linear methods leads to partial analysis, at best, and deception that the problem has been solved" [5, p. 16]. This is a highly significant point when considering K-12+ educational frameworks and practices. It stands to reason that security training and digital literacy taught within the confines of traditional linear methods might create potential deception as the structures for learning might not fully support a security mindset, which is heavily reliant on flexible, dynamic thinking [1]. K-12+ education would thus benefit from a holistic approach, involving the entire system, rather than implementing fragmented fixes [17]. Complexity theory serves as an appropriate lens as the theory shifts focus from reductionism (reducing a system to its individual parts), to the dynamic ways in which individual parts interact and affect each other as a whole [4], [5].

Complexity theory also recognizes similarities between a variety of organizational phenomena and the phenomena found in science and nature [18]. Like nature, organizations are composed of ecosystems and include independent parts that simultaneously rely on one another [19]. While each part of an ecosystem competes for survival, from a system-wide perspective it is apparent each part needs "others in order to survive and thrive in the ecosystem… each pair of (inter)dependencies [has] to co-evolve—the entire system [develops] these relationships across networks, all at once over time" [19, p. 1]. Ecosystems may assist in our thinking about societal resilience and the potential power of interdependence in the forming of a security mindset. Lichtenstein further affirms the ways in which,

> dynamic interactions and relationships across the entire ecosystem have generated a resilience, an increased ability of the system as a whole to support the organisms within it. This systemic property of resilience is emergent, for it is not "in" any one element or species but arises through the interactions and relationships across all of them. The same can be said for organizations as emergent systems. [19, p. 2]

V. Pedagogical Misalignment

When addressing whether it is possible for students to learn the skills needed for a security mindset, Dark states it is possible for students "to recognize and respond to complex, emergent behavior," but not if they are taught within the "traditional mode of didactic instruction" [20, p. 61]. Education is in need of reinvention [7] and a diffusion of complexity that shifts beyond a sole reliance on traditional methods of schooling [21].

Although many scholars, for literally over a century [11], [22], [23] have challenged the overreliance on traditional methods, a majority of attempts at reform have been "hopelessly constrained within an instrumental rationality" [17, p. 101], representing "tweaks and intensifications of existing policies" rather than "wholesale redesigns" [24, p. 121-122]. Complexity has the potential to "open a space to rethink curriculum and pedagogy as an organic and living process that is connected to place, community, and local knowledge" [17, p. 101]. This philosophy aligns well with the CSC's call for public awareness and civic education [9] in recognition of the vigorous relationship between security and civic interdependence. Social and cultural factors are key to security [1]. Hence, an education rooted in complexity holds dynamic possibilities for civic education and a sense of community and place, further emphasizing security as a social act.

In the following sections, we address the most prominent, pedagogical frameworks and practices in need of redesign rather than temporary reforms, highlighting the ways in which a monolithic adherence to each potentially poses threats to security.

A. *Rigid, Prescriptive Curricula*

Emergence rises out of complexity. Emergence has been defined as the "coming into being" [19, p. 158] "of new processes, structures, and entities" [4, p. 2]. Like traditional science that relies heavily on predictability, planning, and linearity [4], [5], traditional K-12+ relies heavily on explicit answers and prescriptive assignments. Yet organizations, such as technology companies, take a flexible approach to continuous change, and are able to shape emergence through strategic design and adaptiveness, both of which are essential to success [4]. Conventional planning on the other hand has been proven less effective than designing for emergence [4]. As Yorks and Nicolaides state, the "illusion of predictability is being unmasked" [25, p. 58]. This does not dismiss the fundamental building blocks necessary to learning; it is an urgent request that the fundamentals serve as a part of learning, rather than the absolute center of learning. K-12+ education systems employ frameworks and practices primarily rooted in predictability but neglect to supplement learning with skills that equip students to adapt to uncertainty. As Nicolaides and Yorks appropriately describe:

> Even as our knowledge base in terms of seeing learning as a noun is becoming more and more rich, our sense of control over our world is becoming less. It is as if we are becoming less knowing even as we become more knowledgeable. Addressing this paradox, we suggest, requires that we look at the process of learning, and take seriously the implications of understanding learning as a verb. [25, p. 50]

K-12+ education often promotes the implementation of rigid, prescriptive curricula [26], [27] that often takes the form of a set of predictable, linear exercises leading to predetermined assessments and fixed knowledge that dictate the flow of the classroom more so than human factors such as meaningful interactions and basic understanding [7], [17], [24]. For example, even most classroom science experiments end with dutifully logged answers rather than genuine, unpredictable outcomes that evoke further, deeper inquiry [24], [28] and emergent qualities. Consider how many assignments culminate in a one-time presentation, an essay, or an exam. Contrarily, a flexible curriculum, with less reliance on linearity and predictability, would open up opportunities for emergence for educators and students alike [17], [21], [24].

This is not to suggest a free-for-all mentality without classroom structure or essential knowledge but rather a shift toward strategic design, allowing for flexible environments that evolve through authentic interplay between people, environments, situations, and the learning itself [5], [7], [21]. Byrne refers to this as the "Pedagogy OF Complexity" in which complexity thinking is diffused within classrooms, adding contextual layers as students apply their learning to create unpredictable yet strategic, emergent outcomes [21, p. 40]. Byrne uses the example of problem-based learning in which students apply their learning to a problem [21]; in turn the context provides deeper, more emergent and collaborative outcomes, placing creativity in the hands of students rather than the curriculum developers'.

Making this shift is a difficult process for many teachers who were themselves exposed to rigid, prescriptive curricula and now teach in a similar fashion, finding it highly difficult to step away from that mindset [24], [26], [29]. Often teachers must "unlearn" traditional practices, which can take years even for successful teachers [26]. Enright et al. address a similar concern when describing the antiquated university structure, producing tension between the static nature of cybersecurity programs and the dynamic, ever changing nature of cybersecurity [8].

When taking into consideration the mass amounts of end users exposed to consistent linearity and predictability found within traditional schooling, it is reasonable to question the level of "unlearning" that must occur when adapting to today's socio-technical systems of which are "complex and the outcomes thereof emergent, indeterminate and unpredictable" [2, p. 176]. Much of today's core classrooms, often absent deeper learning, voice, and creativity [24], [26], leave students exposed to prescriptive curricula even though one's relationship "with ambiguity is a critical factor, for ambiguity is what one confronts in making choices for which the impact cannot be determined with any degree of certainty" [30, p. 185]. In essence, rigid curricula reinforce predictability, instead of fostering opportunities for students and educators to manage ambiguity and develop adaptability which are central skills to cybersecurity. A security mindset requires that end users remain aware of "new threats and new protective measures" [1, p. 7] in response to ever changing technology and complexity.

Cyber experts make parallel claims in reference to cybersecurity education in the workplace, understanding that the training in isolation is ineffective and involves many other socio-technical factors [3], [10], [12]. As Emm illustrates, "Security must become part of the company's wider culture: otherwise, it's like doing the housework once and imagining that this will suffice to keep the house clean" [31, p. 15].

Furthermore, if end users employ security behaviors in one part of their lives but not others, they may develop "a false sense of security" and in time, may revert to insecure habits [31, p. 8]. It is fair to question the implications of rigid, prescriptive curricula within K-12+ education. If not accompanied by daily routines, practices, and flexible frameworks in alignment with a security mindset, cybersecurity lessons and rhetoric are likely to provide the illusion of safety; behind the scenes a rigid, prescriptive curriculum, continues to foster poor habits and deny end users opportunities to consistently build overall resilience.

B. *Binary Thinking, Compliance, and Standardized Assessments*

Complex thinkers grasp the reality of unpredictable emergence and perpetual learning [17], a skill held in high regard in cybersecurity as cyber specialists call for mental agility and continuous research to manage evolving cyber landscapes [1], [3], [12]. Yet, prevailing educational frameworks and practices often lead students to predetermined outcomes [24], [26] and are less likely to offer open-ended challenges that Schneier suggests assist in the development of a security mindset [32].

McLeod & Shareski declare, "We have overvalued the importance of students giving answers and undervalued the potential of students asking questions... opportunities for genuine inquiry are rare" [24, p. 29]. This poses a security risk, as healthy skeptical metacognition, vital to cybersecurity, is "always alert, questioning, and assessing one's own cognitive activities and performance" [3, p. 306]. Rather than fostering healthy skepticism and insightful questioning, education tends to foster habits of compliance [24], [26]. The mechanical nature of classrooms comes at an expense. Mihaly Csikszentmihalyi, founder of flow theory states, "One of the major functions of every culture has been to shield its members from chaos, to reassure them of their importance and ultimate success… The unwarranted sense of security sooner or later results in a rude awakening" [33, p. 41-42]. For example, if end users "are unaware of their computers or smartphones being compromised, and their experiences are overall positive, their trust in using the internet can grow, despite real threats" [1, p. 7]; therefore, end users would benefit from opportunities to build a mindset in which critical thinking and questioning outweigh compliance.

The culture of compliance finds fuel in standardized assessments. Although students face a highly dynamic society, standardized assessments promote binary thinking (yes/no, if/then, correct/incorrect, cause/effect) which has been coined as the "path to least resistance for human thinking and perceiving" [34, p. 24]. Standardized assessments remain a central measurement for knowledge although "standardized tests may actively discourage the exact type of mental flexibility individuals need to be effective in the ever-changing cyber domain" [12, p. 9]. Furthermore, technology is moving at a rate far faster than academia [13]; yet students are often measured on the content they consume, although the complex nature of cybersecurity demands cognitive models for ongoing researching and learning [12].

The dynamic, flexible, adaptive, and evolving skills imperative to security and complex systems are not considered in the formula designed to measure the best high schools in the United States. This is highly concerning when considering the number of end users and future cyber professionals graduating from the U.S. education system, not to mention the past generations taught in a similar fashion. The 2021 "U.S. News Best High Schools Rankings" uses a methodology that is entrenched in assessments [35]. Despite any of the top schools' innovative offerings, the deeply-rooted nature of standardized testing remains locked inside a traditional framework that promotes and praises the ability to answer questions [24]. This comes at an expense to our security given the binary nature of standardized assessments within a dynamic, ever changing society. As U.S. government agencies scramble to defend U.S. cyber interests, decades of end users, collectively raised with binary thinking, have migrated to a collective, highly complex virtual space. It is fair to question in what ways practices that promote answering and standardized assessments have for decades quite possibly served as contributors to human error, a significant source of adverse cyber incidents [2], [3]. The conflict between standardized assessments and the mental agility required in cybersecurity potentially produces an unproductive, cyclical loop: a number of government agencies defend networks from cyber attacks while the Department of Education enforces parameters and policies that contribute to cyber risks.

C. *Disciplinary Constraints*

Traditional science, heavily reliant on reductionist frameworks, had its place in the past but is inadequate when addressing today's complex issues [5], [7]. Complexity expands on reductionism, emphasizing not only a need to understand each part but to more comprehensively see the parts as they interact as a whole [5]:

> Research suggests that deep learners have schemas that enable them to see how discrete pieces of knowledge in a domain are connected; rather than seeing isolated facts, they see patterns and connections because they understand the underlying structures of the domain they are exploring. [26, p. 12]

Many scholars recognize that dynamic, social systems operate more like ecosystems [5]; hence, they suggest a shift away from reductionist research to embrace a more dynamic society that calls for interdisciplinary competence. Interdisciplinary competence is defined as:

> the ability to think about... [and] use different disciplinary perspectives in solving interdisciplinary problems by making connections, to synthesize and integrate knowledge across academic fields, and the ability to recognize the need to reconsider the direction of one's thinking and problem solving approaches. [36, n.p.]

Interdisciplinary competence is also significant to cybersecurity. For example, interdisciplinary teaming is critical to cybersecurity and the multifaceted nature of the cyber domain, requiring dynamic thinking and behaviors [10], [12]. Because hackers think beyond linear processes, "defenders need to be interdisciplinary in order to take in account various techniques and combat" [10, p. 4]. Furthermore, interdisciplinary competence is not restricted to disciplines but also includes integration of "information, data, techniques, tools, perspectives, concepts, and/or theories… to craft products, explain phenomena, or solve problems" in ways that are impossible with only a single discipline [37, p. 289].

It is important that education systems move in a similar direction; nevertheless, educational structures typically involve disciplinary constraints: "When schools segregate subject areas into disconnected forty-five-minute blocks of time, students' ability to associate across different academic areas is at best an anomaly" [24, p. 77]. This means in addition to the linear, prescriptive curricula previously mentioned, students often receive that curriculum in disciplinary boxes. When considering that educators at times struggle to make and find value in connections between disciplines [24] and “cybersecurity programs tend to exist in academic silos in higher education,” [8, p. 3] it appears evident that decades of confined thought within disciplinary frameworks have fostered reductionist mindsets proven difficult to break today. Exposure to interdisciplinary learning is significant to security, making it important to cultivate interdisciplinary competence at the K-12+ levels. Consequently, the hope is that end users will one day avoid the need to “unlearn” the mental constrictions cultivated within a reductionist mindset in order to better address dynamic cyber threats.

VI. Conclusion

In this paper, we argued for the need to better equip end users with a security mindset due to the realities of increased complexity in today’s hyperconnected world. Accordingly, we propose that end users would benefit from consistent, holistic, daily routines that complement an overarching security mindset and build societal resilience. While we affirm that K-12+ education systems have the potential to support this kind of shaping of security mindsets, we also recognize that K-12+ education systems would first need to overcome systemic misalignment between traditional educational frameworks and practices and the complex nature of an evolving society. In support of this aspiration, we offered an examination of some of the most prominent traditional pedagogical frameworks and practices that we believe stand in conflict with the cultivation of a security mindset. These include: rigid, prescriptive curricula; binary thinking, compliance, and standardized assessments; and disciplinary constraints. At this critical juncture in human history in which socio-technical systems are dramatically transforming the realities of everyday life, K-12+ education systems have the opportunity to design for emergence in support of building a more secure society.

References

[1] W. Dutton, “Fostering a security mindset,” *Internet Policy Review*, vol. 6, no. 1, 2017. [Online] https://doi.org/10.14763/2017.1.443

[2] V. Zimmermann and K. Renaud, “Moving from a ‘human-as-problem’ to a ‘human-as-solution’ cybersecurity mindset,” *International Journal of Human-Computer Studies,* vol. 131, 2019, pp. 169-187. [Online]. Available: https://doi.org/10.1016/j.ijhcs.2019.05.005

[3] K. Neville, et al., “Training to instill a cyber-aware mindset,” *13th International Conference on Human-Computer Interaction*, Orlando, FL, USA, July 26–31, 2019. [Online]. Available: https://doi.org/10.1007/978-3-030-22419-6_21

[4] D. Nijs, “Introduction: Coping with growing complexity in society," *World Futures*, vol. 71, no. 1-2, 2015, pp. 1-7. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/02604027.2015.1087223

[5] J. Turner and R. Baker, “Complexity theory: An overview with potential applications for the social sciences,” *Systems*, vol. 1 , no. 4, 2019. [Online]. Available: https://doi.org/10.3390/systems7010004

[6] B. Schneier, *Click here to kill everybody*. New York City: W.W. Norton Company, 2018.

[7] T. Jörg, “On reinventing education in the age of complexity: A Vygotsky-inspired generative complexity approach,” *Complicity, An International Journal of Complexity and Education*, vol. 14, no. 2, 2017, pp. 30-53. [Online]. Available: https://doi.org/10.29173/cmplct29334

[8] E. Enright, et al., “Building Capacity for Systems Thinking in Higher Education Cybersecurity Programs,” *Journal of The Colloquium for Information Systems Security Education*, vol. 8, no. 1, Fall 2020. [Online]. Available: https://www.researchgate.net/publication/346925406_Building_Capacity_for_Systems_Thinking_in_Higher_Education_Cybersecurity_Programs

[9] A. King and M. Gallagher, *United States of America Cyberspace Solarium Commission*, 2020. [Legislative Proposal]. [Online]. Available: https://www.solarium.gov/report/legislative-proposals

[10] R. Ait Maalem Lahcen, B. Caulkins, R. Mohapatra, M. Kumar, “Review and insight on the behavioral aspects of cybersecurity,” *Cybersecurity*, vol. 31, no. 10, 2020. [Online]. Available: https://doi.org/10.1186/s42400-020-00050-w

[11] L. S. Vygotsky, *Educational psychology*. Boca Raton, FL: St. Lucie Press. (Original work published 1926), 1997.

[12] J. Dawson and R. Thomson, “The future cybersecurity workforce: Going beyond technical skills for successful cyber performance,” *Frontiers in Psychology*, 2018. [Online]. Available: https://doi.org/10.3389/fpsyg.2018.00744

[13] A. Webb, *The big nine: How the tech titans and their thinking machines could warp humanity*, New York City: PublicAffairs, 2019. [E-book] Available: Kindle.

[14] A. J. Crum, P. Salovey, and S. Achor, “Rethinking stress: The role of mindsets in determining the stress response,” *Journal of Personality and Social Psychology*, vol. 104 no. 4, 2013, pp. 716–733. [Online]. Available: https://doi.org/10.1037/a0031201

[15] J. Dewey, *Human nature and conduct*. Courier Corporation, (Original work published in 1922), 2002.

[16] C. Costello, “The promise and peril of our quantum future,” *TED*, 2019. [Online Video].

[17] A. Ovens and J. Butler, “Complexity, curriculum and the design of learning systems,” In *Routledge Handbook of Physical Education Pedagogies*, 2016.

[18] T. Sammut-Bonnici, “Complexity theory” in *Wiley Encyclopedia of Management*, [online document], 2015.

[19] B. Lichtenstein, *Generative emergence*. New York City: Oxford Press, 2014.

[20] M. Dark, “Thinking about cybersecurity.” *IEEE Security & Privacy*, vol. 13, no. 1, 2015, pp. 61-65. [Online] Available: https://ieeexplore.ieee.org/document/7031840

[21] D. Byrne, “Thoughts on a Pedagogy OF Complexity,” *Complicity: An International Journal of Complexity and Education*, vol. 11, no. 2, 2014. [Online]. Available: https://files.eric.ed.gov/fulltext/EJ1074496.pdf

[22] J. Dewey. *Democracy and Education*. New York: Macmillan, 1916.

[23] T. Wagner, *Creating innovators*. New York: Scribner, 2015.

[24] S. McLeod and D. Shareski, *Different schools for a different world*. Bloomington: Solution Tree Press, 2018.

[25] A. Nicolaides and L. Yorks, “An Epistemology of Learning Through.” *Emergence: Complexity & Organization*, vol. 10, no. 1, 2008. [Online]. Available: https://www.proquest.com/scholarly-journals/epistemology-learning-through/docview/214148382/se-2

[26] J. Mehta and S. Fine, *In search of deeper learning: The quest to remake the American high school*. Cambridge: Harvard University Press, 2019.

[27] V. Talanquer, R. Bucat, R. Tasker, P. Mahaffy, “Lessons from a pandemic: Educating for complexity, change, uncertainty, vulnerability, and resilience,” *Journal of Chemical Education*, vol. 7, no. 9, 2020, pp. 2696-2700. [Online]. Available: https:doi.org/10.1021/acs.jchemed.0c00627

[28] T. Wagner, *The global achievement gap: Why even our best schools don’t teach the new survival skills our children need—and what we can do about it*. New York: Basic Books, 2008.

[29] E. Bloom and K. VanSlyke-Briggs, “The demise of creativity in tomorrow’s teachers,” *Journal of Inquiry & Action in Education*,

vol. 10, no. 2, 2019. [Online]. Available: https://digitalcommons.buffalostate.edu/jiae/vol10/iss2/5

[30] L. Yorks and A. Nicolaides, “A conceptual model for developing mindsets for strategic insight under conditions of complexity and high uncertainty,” *Human Resource Development Review*, Vol. 11, no. 2, 2012, pp. 182–202. [Online]. Available: https://doi.org/10.1177/1534484312439055

[31] T. Caldwell, “Making security awareness training work,” *Computer Fraud & Security*, 2016. [Online]. https://doi.org/10.1016/S1361-3723(15)30046-4

[32] C. Severance, “Bruce Schneier: The Security Mindset,” *Computer*, vol. 49, no. 2, 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7404197

[33] M. Csikszentmihalyi, *Flow: The psychology of optimal experience*, New York: Harper Row, 2008.

[34] P. Elbow, “The uses of binary thinking,” *Journal of Advanced Composition*, vol. 13, no. 1, 1993, pp. 51-78. [Online]. Available: https://scholarworks.umass.edu/cgi/viewcontent.cgi?article=1013&context=eng_faculty_pubs

[35] “U.S. News Best High Schools Rankings,” *U.S. News*, 2021. [Online]. Available: https://www.usnews.com/education/best-high-schools/articles/how-us-news-calculated-the-rankings

[36] M. Brassler and J. Dettmers, “How to enhance interdisciplinary competence – interdisciplinary/problem-based learning versus interdisciplinary,” *Interdisciplinary Journal of Problem-Based Learning*, vol. 11, no. 2, 2017. [Online]. Available: https://doi.org/10.7771/1541-5015.1686

[37] V. Boix Mansilla, “Learning to synthesize: the development of interdisciplinary understanding,” In *The Oxford Handbook of Interdisciplinarity*, Oxford: Oxford University Press, 2010, pp. 288-306.