

A Deweyan Foundation for Cultivating Reflective Cyber-Attuned Habits in an Age of AI and Ambiguity

Jane Blanken-Webb
Alley School of Education
Wilkes University
Wilkes-Barre, PA, USA
jane.blankenwebb@wilkes.edu
0000-0003-4656-5739

Abstract—Rapid advances in AI, automation, and hyperconnectivity are outpacing human habits, producing pervasive ambiguity. Drawing on John Dewey’s philosophy of habit as growth through disruption and inquiry, this paper reconceptualizes cybersecurity education as cultivating reflective, cyber-attuned habits across society—not only training specialists. Dewey’s account of growth through disruption, inquiry, and reorganization are translated into three educational design moves: (1) embed reflective inquiry within procedural exercises; (2) employ inquiry-based, experiential formats (e.g., capture-the-flag, cyber-defense exercises, cyber-ranges) to practice reasoning under uncertainty; and (3) extend learning to social practices of verification and shared deliberation beyond technical settings. The approach turns error into material for growth and equips learners to act with intelligent adaptability. Rather than proposing a fixed framework, the paper offers a conceptual position grounded in Deweyan philosophy, highlighting design implications that can inform educational practice across varied contexts.

Keywords—*cybersecurity education, John Dewey’s philosophy, habit, growth*

I. INTRODUCTION

Educators today are preparing learners for an environment in which the rapid pace and proliferation of technological advancement are producing profound ambiguity and uncertainty that none of us within the learning ecosystem is fully equipped to confront. More than a century ago, John Dewey grappled with a similar challenge of education in times of upheaval. He argued that when environments undergo significant change, human habits inevitably lag behind, making it essential for education to cultivate the capacity for intelligent growth amid disruption [1]–[5]. Dewey wrote in the context of industrialization and mass communication, where established assumptions and ways of life were being reorganized at unprecedented speed. Today, AI, automation, and hyperconnectivity present an analogous challenge: environments are evolving faster than the habits, practices, and assumptions that guide human behavior.

In cybersecurity education, this gap is especially consequential and far-reaching. While much of the field’s emphasis rightly focuses on preparing technical professionals to defend critical systems, these same challenges of ambiguity and adversarial conditions extend well beyond the cyber workforce. Across workplaces and communities, people now inhabit a shared digital ecosystem—and all are vulnerable in ways that require cultivating adaptive, reflective, cyber-attuned habits [6]. Thus, the focus of this paper is to reconceptualize cybersecurity education to include the cultivation of such habits across society, drawing on Dewey’s theory of habit as a foundation for preparing learners to adapt intelligently in the face of technological disruption. I contend that Dewey’s philosophy of habit equips cybersecurity education to meet the challenges of AI, automation, and hyperconnectivity by clarifying how reflective inquiry reorganizes habit into reflective practice attuned to the fluid, AI-mediated uncertainties of contemporary cyberspace. Such habits do more than mitigate the risks of error; they empower learners to be response-able—to pause, deliberate, and act with intelligent adaptability, even when mistakes are part of the process of growth [2].

The paper proceeds in four sections. Section II characterizes the contemporary challenge for cybersecurity education as the accelerating interplay of AI, hyperconnectivity, and automation, illustrating how deepfakes, expanding Internet of Things (IoT) attack surfaces, and cyber-physical interdependencies unsettle human judgment and expose the limits of procedural-only training. Section III develops Dewey’s account of habit as growth through disruption, inquiry, and reorganization, clarifying how mistakes become materials for intelligent adaptation in digital contexts. Section IV offers three design moves for cultivating reflective, cyber-attuned habits across society: (1) embed reflective inquiry within procedural exercises, (2) employ inquiry-based, experiential formats (e.g., CTFs, cyber defense exercises, cyber-ranges) to practice reasoning under uncertainty, and (3) extend learning to social practices of verification and shared deliberation beyond strictly technical settings. Section V draws implications for course, assessment, and program levels and concludes by positioning cybersecurity education not only as workforce preparation but

as a conceptual orientation for cultivating adaptive habits essential to resilience in an age of AI and ambiguity.

II. CYBERSECURITY EDUCATION IN THE AGE OF AI AND AMBIGUITY

Cybersecurity education faces a profound challenge in preparing learners for environments defined by constant disruption. The ambiguity learners encounter today stems less from any single technological development than from the accelerating interplay of AI, hyperconnectivity, and automation, which generate adversarial conditions at a pace that outstrips established practices and assumptions [7]–[9]. In such contexts, the vulnerabilities extend beyond technical systems to include human judgment, social trust, and public life.

AI-generated disinformation illustrates this challenge clearly. Deepfakes and synthetic media increasingly blur the boundaries between fact and fabrication, eroding confidence in information ecosystems and demanding new habits of verification from all participants [7]. Similarly, the rapid proliferation of IoT devices has expanded the attack surface in ways that are both technically complex and socially opaque. Recent studies show that vulnerabilities in IoT platforms and device protocols continue to emerge despite years of research and standardization efforts, leaving individuals and organizations exposed in unexpected ways [8]. At a broader scale, cyber-physical infrastructures now link digital vulnerabilities with physical consequences. The President's Council of Advisors on Science and Technology (PCAST) has emphasized that the resilience of critical systems increasingly depends on human capacity to adapt to adversarial disruptions that cannot be fully anticipated [9].

Traditional approaches to cybersecurity education emphasize technical proficiency and procedural compliance—critical skills for protecting infrastructure and data. Yet these approaches alone are insufficient for the challenges posed by AI-driven ambiguity and hyperconnected systems. Procedural training prepares learners for known threats but cannot anticipate novel attack vectors or adversarial strategies designed to exploit human assumptions. For example, password policies, patch management, and phishing simulations build useful defensive routines, but they risk instilling a false sense of security when learners equate compliance with preparedness [10]. The field has begun to recognize this limitation by calling for more emphasis on adaptability, socio-technical awareness, and human agency in cybersecurity education [11], [12].

Cybersecurity education, therefore, must not only train specialists but also cultivate habits of mind that enable all learners to navigate uncertainty. Ordinary users, professionals

in non-technical fields, and community members are increasingly entangled in digital environments where trust can be manipulated, information weaponized, and vulnerabilities rapidly exploited. Meeting this challenge requires pedagogical approaches that prepare learners to act intelligently amid ambiguity, reshaping their habits in response to disruption rather than relying solely on prescriptive procedures.

III. HABIT IS GROWTH THROUGH DISRUPTION: A DEWEYAN LENS

To address the challenges of AI and ambiguity, I turn to John Dewey's account of habit as developed throughout his middle and later works. Dewey's understanding of habit differs meaningfully from the everyday notion of routine or mechanical repetition. In *Human Nature and Conduct* (1922) [1], he describes habits as dynamic, projective patterns of conduct that emerge in continuous transaction with the environment. A habit, for Dewey, is less a fixed routine than an "art formed through past experience" [1, MW 14: 481¹], valuable not for its repetition but for its ability to adapt and conduct intelligently amid the disruptions of the present moment.

Dewey situates habit within an environment that is always changing. When established habits prove insufficient for new conditions, disruption gives rise to the release of impulse—a blind surge of energy that signals misalignment between organism and environment. Yet impulse alone is not intelligent; it must be taken up by reflection through exploring considerations of possible actions. In this process, prior habits are tested against the particulars of the situation until a course of action is selected [1, MW 14: 132–134]. Once enacted, the consequences of this action are revealed within the situation, and the experience becomes incorporated into the repertoire of past conduct available for future reflection—sometimes reinforcing existing habits, and at other times reorganizing them into new ones. In this sense, habit is never static but always subject to growth through disruption. This continual cycle of disruption, reflection, and reorganization means that mistakes are not simply failures but integral signals that prompt growth and reorientation. Thus, for education, what matters is not the avoidance of mistakes but the cultivation of capacities for intelligent reorganization when mistakes inevitably occur. For a fuller treatment of this Deweyan cycle applied to cybersecurity contexts, see [6].

Dewey's account of habit as growth through disruption and intelligent reorganization is particularly relevant for cybersecurity education. Learners often encounter environments where adversarial conditions evolve faster than prior knowledge can adapt—whether through AI-generated disinformation, unexpected IoT vulnerabilities, or novel attack vectors [6]–[8]. Procedural knowledge alone, while necessary,

1. Dewey citations follow the standard convention in Dewey scholarship: the Boydston Collected Works of John Dewey, 1882–1953 (Southern Illinois University Press). Citations use the abbreviations MW (Middle Works), and LW (Later Works), followed by volume and page (e.g., MW 14: 132–134). Full bibliographic entries appear in the reference list.

cannot anticipate the full range of disruptions learners will face. Dewey's conception of habit emphasizes the ongoing interplay between environment, impulse, and reflection, highlighting the importance of preparing learners to develop reflective, cyber-attuned habits that enable intelligent action amid conditions they cannot fully predict.

Dewey also contrasts "good" and "bad" habits not by their frequency or ease of performance but by their responsiveness to new conditions. Habits that are enslaved to "old ruts" become maladaptive, while those that remain available for "new emergencies" sustain growth [1, MW 14: 48]. In the context of cybersecurity, this distinction speaks to the difference between rote procedural compliance and reflective, adaptive engagement. Compliance-oriented routines—such as mandatory password resets or patching policies—are valuable for known threats, but when treated as sufficient, they risk instilling rigidity that adversaries can exploit [10], [11]. Reflective, cyber-attuned habits—habits that pause, question, and deliberate—are far better suited to fluid and adversarial environments.

In *Democracy and Education* (1916) [2], Dewey makes this educational imperative explicit. He argues that education should not merely transmit settled knowledge but cultivate "the discernment of the relationship between what we try to do and what happens in consequence" [2, MW 9: 151]. This orientation fosters responsibility by engaging learners in the consequences of their actions, preparing them to adapt intelligently rather than repeat procedures mechanically. Likewise, in *Art as Experience* (1934) [4], Dewey describes the educative value of experience as a process of doing and undergoing, in which reflective struggle transforms raw impulse into intelligent action [4, LW 10: 42–63]. These accounts converge on the idea that habits formed through reflective inquiry are the basis of growth in uncertain conditions.

Finally, in *The Quest for Certainty* (1929) [5], Dewey critiqued the philosophical impulse to treat uncertainty as a defect to be overcome, urging instead the pursuit of "security by practical means in place of [the] quest of absolute certainty by cognitive means" [5, LW 4: 20]. From this perspective, cybersecurity education should be cautious about granting learners a false sense of certainty in digital environments and instead foster the capacity to act intelligently amid ambiguity. This entails cultivating habits of reflective adjustment—practices of questioning, verifying, and reorganizing—that sustain agency even when error and disruption are unavoidable.

In sum, Dewey's philosophy of habit reframes the challenge of cybersecurity education in the age of AI and ambiguity. Building on existing efforts to prepare technical specialists, this perspective broadens cybersecurity education by emphasizing that all learners need reflective, cyber-attuned habits capable of adapting intelligently in the face of disruption. By embracing error as a condition of growth and by fostering habits responsive to new conditions, educators can

better equip learners to navigate the profound uncertainties of today's technological landscape.

IV. RECONCEPTUALIZING CYBERSECURITY EDUCATION THROUGH A DEWEYAN LENS

Cybersecurity education is already evolving to address the challenges of environments shaped by AI, automation, and hyperconnectivity. Recent work in cybersecurity education highlights how curricula are being restructured, integrating AI-focused training and emphasizing interdisciplinary collaboration to prepare students for these conditions [12], [13]. Guided by Dewey's view that habits grow through disruption and reflective adjustment, this section shows how to design learning to cultivate reflective, cyber-attuned habits, offering three concrete approaches for fluid, AI-mediated conditions. Rather than replace current practice, these proposals provide a conceptual foundation for broadening cybersecurity education's scope and impact.

A. From Procedural Compliance to Reflective Inquiry

Cybersecurity education has long relied on procedural training—whether through phishing simulations, compliance checks, or policy-driven exercises—as a means of instilling defensive routines. These approaches are essential for building baseline competencies, but research has shown that when treated as sufficient, they risk producing narrow forms of compliance rather than fostering adaptive awareness. Jansson and von Solms, for example, argue that while phishing simulations can increase short-term awareness, they often fail to produce lasting behavioral change if learners are not engaged in deeper reflection about why they were deceived [14]. Similarly, Parsons *et al.* demonstrate that security awareness measured through checklists and questionnaires captures only surface-level compliance and does not necessarily reflect learners' ability to respond intelligently in novel situations [15]. Dewey's philosophy of habit provides a conceptual foundation for addressing this limitation. Rather than viewing procedures as endpoints, educators can frame them as occasions for inquiry. For instance, a phishing simulation can do more than train learners to detect specific cues; it can serve as a starting point for reflection on how adversaries exploit habits of trust, attention, and urgency. By embedding procedural exercises within reflective inquiry, cybersecurity education can help learners cultivate habits that remain flexible and adaptive under unpredictable conditions.

B. Inquiry-Based Experiential Learning

A Deweyan stance treats procedures not as endpoints but as starting points for inquiry—learners test possibilities, observe consequences, and reorganize their habits accordingly. Cybersecurity programs are already moving in this direction as part of broader AI-era curriculum shifts [13]. Inquiry-oriented, hands-on formats such as Capture-the-Flag (CTF), cyber defense exercises, and competitions place learners in uncertain, adversarial scenarios where they must meet problematic situations through inquiry—imaginatively

rehearse possible lines of action and test consequences—rather than execute fixed routines [16]–[18]. Studies report higher engagement, stronger confidence, and improved self-assessed skills in these inquiry-driven contexts, while also revealing teamwork dynamics and shared situation awareness under realistic pressure [16], [17]. In team settings, realistic cyber defense competitions foster emergent role specialization and coordinated defensive strategies, giving participants practice in collaboration and shared situation awareness—capacities central to acting intelligently amid ambiguity [17]. At the field level, a recent survey shows that cybercompetitions and cyber-ranges have matured into key instructional infrastructures for experiential learning, with design opportunities and challenges aligned with cultivating reflective, adaptive habits rather than checklist compliance [18]. Taken together, these formats operationalize Dewey’s account of “doing and undergoing” by embedding learners in consequential practice and structured reflection [4].

C. *Cultivating Habits for Social as well as Technical Life*

Cybersecurity is not only a technical domain but also a social one in which trust, judgment, and responsibility are continually negotiated in relationships and communities. AI-generated media and platform dynamics can destabilize shared information ecologies, making social trust itself a target and demanding habits of verification and deliberation from all participants—not just specialists [7]. Such habits are relational as well as technical, aligning with care-centered accounts of cybersecurity practice [19]. A Deweyan lens casts these as social practices of inquiry: pausing to question sources, seeking corroboration, and reflecting on likely consequences before acting [2], [4]. Framed this way, cybersecurity education extends beyond workforce preparation to include ordinary users and professionals in non-technical fields, cultivating reflective, cyber-attuned habits that enable intelligent action amid ambiguity. This shift aligns with calls to treat humans as part of the solution in socio-technical security—emphasizing agency, resilience, and adaptive judgment rather than rote compliance [11]—and with current roadmaps for AI-era curricular innovation [13]. It also accords with national guidance that system resilience now depends on human capacity to adapt under unanticipated disruptions [9]. Designing exercises that ask learners to check sources with others, articulate reasons, and reflect before acting enables them to develop the social habits cybersecurity demands as much as the technical ones.

V. CONCLUSION AND IMPLICATIONS FOR PRACTICE

This paper advances a conceptual position rather than a prescriptive framework. Grounded in Deweyan philosophy, it offers a theory-informed orientation toward designing learning experiences that cultivate reflective, cyber-attuned habits. The educational design moves proposed here are not exhaustive or universally applicable; instead, they are intended to guide educators in interpreting and adapting Dewey’s concepts within their own pedagogical and institutional contexts. This paper has argued that Dewey’s account of habit as growth

through disruption, inquiry, and reorganization offers a productive lens for cybersecurity education in conditions shaped by AI, automation, and hyperconnectivity. The lens reframes procedures as occasions for inquiry, elevates experiential formats (e.g., CTFs, cyber defense exercises, cyber-ranges) as habit-forming contexts, and extends cybersecurity beyond technical specialization to include the social practices of verification and shared deliberation.

Translating this account into practice begins with course design. Pairing procedural training with structured reflection turns procedures into occasions for habit formation in Dewey’s sense. Rather than repeating routines, learners develop dynamic, projective capacities formed in transaction with their environment and carefully attuned to specific conditions [1, MW 14: 38, 48, 132–134]. Short post-mortems after labs or simulations (for example, asking “What cues did I trust?”, “Which assumptions failed?”, and “What will I try next time?”) can serve as assumption audits that surface habits adversaries exploit (e.g., urgency, authority, similarity). In addition, prompts that require imaginative rehearsal of options before acting help anchor inquiry at the point of action.

Beyond activity design, assessment should honor learning as a process of coming-to-know rather than a snapshot of right answers. In practice, this means privileging process-level evidence—decision logs, version histories, timing and sequence data, teammate rationales—because such traces capture the *doing and undergoing* of inquiry and make visible how learners frame problems, test and revise hypotheses, coordinate with others, and reorganize habits in light of consequences [20]; cf. [1]–[2], [4]. Read through a Deweyan lens, these artifacts are not peripheral—they are the very materials by which reflective, cyber-attuned habits take shape.

At the program level, inquiry-based, adversarial practice should be threaded throughout the curriculum. Experientially based pedagogies such as CTFs, cyber defense exercises, and cyber-ranges offer chief opportunities to cultivate reasoning under conditions of uncertainty. And in non-technical courses and professional programs, social practices—checking sources with peers and justifying actions before execution—can be embedded to cultivate reflective, cyber-attuned habits across the learning ecosystem. Aligning these moves with emerging AI-era roadmaps in cybersecurity education [13] and with national guidance emphasizing human adaptability for cyber-physical resilience [9] strengthens coherence across courses and programs.

Despite its promise, implementing a Deweyan approach also presents notable challenges that educators must navigate. One key difficulty lies in the time and curricular flexibility required to support structured reflection alongside technical training. Deweyan practices often ask learners to engage in inquiry, experimentation, and reflective deliberation—all of which can appear at odds with assessment regimes focused on coverage, compliance, or certification. Instructors may also lack support or training in facilitating

open-ended inquiry in technically demanding domains, where outcomes are often judged by right answers or known exploits. Furthermore, institutional pressures toward standardization can make it difficult to prioritize experiential learning and reflection over repeatable, testable procedures. These tensions do not invalidate the approach but instead highlight the need for thoughtful integration—such as pairing inquiry with procedural content, embedding reflection within existing formats, and developing institutional norms that value process-based evidence of learning. By acknowledging these constraints, educators can more realistically adapt Dewey's vision within the practical demands of cybersecurity education.

More than a century after Dewey diagnosed the lag between rapidly changing environments and the habits that guide human action, the same pattern marks today's AI-suffused, hyperconnected world. The task before cybersecurity education is not to promise certainty but to cultivate reflective, cyber-attuned habits that help learning keep pace with change—habits formed through inquiry, tested in experience, and continually reorganized as conditions shift across workplaces and communities. When classrooms, labs, and training programs are designed with this aim, they become places where technical practice and reflective judgment grow together, equipping people to meet ambiguity without paralysis and adversarial pressure without rigidity. Designed this way, learning can prepare people across the ecosystem to turn disruption into inquiry, mistakes into material for growth, and surprise into intelligent action.

ACKNOWLEDGEMENT

A large language model (ChatGPT, OpenAI) was used as a writing aid to draft phrasing, reorganize text, and, in select instances, suggest candidate literature. The author selected, read, and verified all cited references and quotations and retains full responsibility for the content and any errors. No data analysis, figures, or confidential materials were generated or processed by the tool. This disclosure aligns with IEEE guidance on responsible use of generative AI in scholarly publishing.

REFERENCES

- [1] J. Dewey, *Human Nature and Conduct*, vol. 14 of *The Middle Works of John Dewey, 1899–1924*, J. A. Boydston, Ed. Carbondale, IL, USA: Southern Illinois Univ. Press, 1983 [Original work published 1922].
- [2] J. Dewey, *Democracy and Education*, vol. 9 of *The Middle Works of John Dewey, 1899–1924*, J. A. Boydston, Ed. Carbondale, IL, USA: Southern Illinois Univ. Press, 1980 [Original work published 1916].
- [3] J. Dewey, *Freedom and Culture*, vol. 13 of *The Later Works of John Dewey, 1925–1953*, J. A. Boydston, Ed. Carbondale, IL, USA: Southern Illinois Univ. Press, 1989 [Original work published 1939].
- [4] J. Dewey, *Art as Experience*, vol. 10 of *The Later Works of John Dewey, 1925–1953*, J. A. Boydston, Ed. Carbondale, IL, USA: Southern Illinois Univ. Press, 1987 [Original work published 1934].
- [5] J. Dewey, *The Quest for Certainty*, vol. 4 of *The Later Works of John Dewey, 1925–1953*, J. A. Boydston, Ed. Carbondale, IL, USA: Southern Illinois Univ. Press, 1984 [Original work published 1929].
- [6] J. Blanken-Webb, H. Hanna, and A. Kuiken, "Cyber education: A Deweyan foundation for security mindset," in *Centennial Handbook on John Dewey's Human Nature and Conduct*, L. J. Waks and A. R. English, Eds. Cambridge, UK: Cambridge Univ. Press, 2026, pp. 201–215.
- [7] R. Chesney and D. K. Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *Calif. Law Rev.*, vol. 107, no. 6, pp. 1753–1820, Dec. 2019.
- [8] H. I. Ahmed, A. A. Nasr, S. Abdel-Mageida, and H. K. Aslan. "A Survey of IoT Security Vulnerabilities and Defenses," *International Journal of Advanced Computer Research*, Vol 9, no. 45, pp. 325–350, Nov. 2019. DOI: 10.19101/IJACR.2019.940116.
- [9] President's Council of Advisors on Science and Technology (PCAST), *Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital World*. Executive Office of the President, Feb. 2024. [Online]. Available: https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/PCAST_Cyber-Physical-Resilience-Report_Feb2024.pdf
- [10] M. Dark, "Thinking About Cybersecurity," *IEEE Security Privacy*, vol. 13, no. 1, pp. 61–65, Jan.–Feb. 2015, doi: 10.1109/MSP.2015.17.
- [11] V. Zimmermann and K. Renaud, "Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset," *Int. J. Human-Comput. Studies*, vol. 131, pp. 169–187, 2019, doi: 10.1016/j.ijhcs.2019.05.005.
- [12] M. Roshanaei and M. Jachura, "Integrating AI in Cybersecurity Higher Education: A Path to Workforce Readiness," *Journal of Intelligent Learning Systems and Applications*, vol. 17, no. 2, pp. 45–67, 2025, doi: 10.4236/jilsa.2025.172005.
- [13] V. Heydari and K. Nyarko, "Empowering the Next Generation: A Strategic Roadmap for AI in Cybersecurity Education," *Journal of the Colloquium for Information Systems Security Education (CISSE)*, vol. 12, no. 1, pp. 1–14, 2025, doi: 10.53735/cisse.v12i1.202
- [14] K. Jansson and R. von Solms, "Phishing for phishing awareness," *Behaviour and Information Technology*, vol. 32, no. 6, pp. 584–593, 2013, doi: 10.1080/0144929X.2011.632650.
- [15] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, T. Zwaans, "The human aspects of information security questionnaire (HAIS-Q): Two further validation studies," *Computers and Security*, vol. 66, pp. 40–51, May 2017, doi: 10.1016/j.cose.2017.01.004.
- [16] K. Leune and S. J. Petrilli, "Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education," in *Proc. 18th Annual Conference on Information Technology Education (SIGITE)*, 2017, pp. 47–52, doi: 10.1145/3125659.3125686.
- [17] N. Buchler, C. G. La Fleur, B. Hoffman, P. Rajivan, L. Marusich, and L. Lightner, "Cyber Teaming and Role Specialization in a Cyber Security Defense Competition," *Frontiers in Psychology*, vol. 9, art. 2133, Nov. 2018, doi: 10.3389/fpsyg.2018.02133.
- [18] T. Balon and I. (Abe) Baggili, "Cybercompetitions: A Survey of Competitions, Tools, and Systems to Support Cybersecurity Education," *Education and Information Technologies*, vol. 28, no. 9, pp. 11759–11791, Sep. 2023, doi: 10.1007/s10639-022-11451-4.
- [19] J. Blanken-Webb and R. Cloutier, "Cybersecurity and the ethics of care," *Information Security Education Journal*, vol. 7, no. 2, pp. 31–39, 2020, doi: 10.6025/isej/2020/7/2/31-39. Available: https://www.dline.info/isej/fulltext/v7n2/isejv7n2_1.pdf.
- [20] J. Blanken-Webb, "Big data's call to philosophers of education," *Philosophical Inquiry in Education*, vol. 24, no. 4, pp. 310–322, 2017, doi: 10.7202/1070689ar.